Harris County Information Technology

Received & Inspected

AUG 11 2010

FCC Mail Room

August 10, 2010

From the desk of:

John Chaney

Sr Technologist

Harris County Information Technology

Bruce High CIO

To the members of the FCC waiver consideration group,

Please accept our waiver request. The Harris County BIGNET group would like to thank you for this opportunity to serve public safety. We would also like to applaud you on your effort to encourage interaction and collaboration between agencies and government that to this day have functioned independent. This effort will result in a better world for the public safety sector and correspondingly a better world for the public and private sector.

Thank You,

John Chaney

No. of Copies rec'd 1
List A B C D E

HARRIS COUNTY, TEXAS

Information Technology Center

Bruce High
Chief Information Officer

10 AUG -4 AM 10: 11
HARRIS COUNTY
MANAGEMENT SERVICES

Vote of the Court:	Yes	No	Abstain
Judge Emmett	☑	☐	☐
Comm. Lee	☑	☐	☐
Comm. Garcia	☑	☐	☐
Comm. Radack	☑	☐	☐
Comm. Eversole	☑	☐	☐

August 4, 2010

Commissioners Court
Harris County Administration Building
1001 Preston, 9th Floor
Houston, Texas 77002

RE: Request permission to submit a 700 MHz Broadband waiver to the Federal Communications Commission (FCC).

Members of Commissioners Court:

The Information Technology Center respectfully requests permission to submit our 700 MHz broadband waiver and supporting documentation to the Federal Communications Commission (FCC). This is in conjunction with the approval that was given to Information Technology Center to submit for the Broadband Technology Opportunities Program (BTOP) in April 2010.

Respectfully submitted,

Bruce High

Bruce High
Chief Information Officer

BH/JC/rlf

Attachments

cc: Ian Gorman, Grant Coordinator – Management Services
Scott Bresk, County Attorney's Office
Craig Bernard, Managing Director – Communications
David Dodson, Division Chief – Communications/Radio
John Chaney – Communications/Radio
Tammie Davidson, Managing Director – Business Operations
Chron

Presented to Commissioner's Court

AUG 10 2010

APPROVE G | L
Recorded Vol_____ Page_____

For Inclusion on Court Agenda dated August 10, 2010.

406 Caroline, 4th Floor / Houston, Texas 77002-2027
Phone 713-755-6621 / Fax 713-755-8930 / www.hcrz.net/itc

Presented to Commissioner's Court

AUG 10 2010

APPROVE_____

Recorded Vol_____Page_____

THE STATE OF TEXAS §
§
COUNTY OF HARRIS §

The Commissioners Court of Harris County, Texas, convened at a meeting of said Court at the Harris County Administration Building in the City of Houston, Texas, on the ____ day of AUG 10 2010 2010, with the following members present, to-wit:

Ed Emmett	County Judge
El Franco Lee	Commissioner, Precinct No. 1
Sylvia R. Garcia	Commissioner, Precinct No. 2
Steve Radack	Commissioner, Precinct No. 3
Jerry Eversole	Commissioner, Precinct No. 4

and the following members absent, to-wit: NONE, constituting a quorum, when among other business, the following was transacted:

ORDER AUTHORIZING THE COUNTY JUDGE TO EXECUTE A REQUEST FOR WAIVER OF THE FCC'S RULES TO ALLOW THE DEPLOYMENT OF A 700 MHZ INTEROPERABLE MOBILE PUBLIC SAFETY BROADBAND NETWORK

Commissioner Garcia introduced an order and made a motion that the same be adopted. Commissioner Lee seconded the motion for adoption of the order. The motion, carrying with it the adoption of the order, prevailed by the following vote:

	Yes	No	Abstain
Judge Ed Emmett	☑	☐	☐
Comm. El Franco Lee	☑	☐	☐
Comm. Sylvia R. Garcia	☑	☐	☐
Comm. Steve Radack	☑	☐	☐
Comm. Jerry Eversole	☑	☐	☐

The County Judge thereupon announced that the motion had duly and lawfully carried and that the order had been duly and lawfully adopted. The order thus adopted follows:

WHEREAS, Harris County desires to request a waiver of the Federal Communications Commission's rules to allow the deployment of a 700 MHz interoperable mobile public safety broadband network.

NOW, THEREFORE, BE IT ORDERED BY THE COMMISSIONERS COURT OF HARRIS COUNTY, TEXAS, THAT:

Section 1: The recital set forth in this Order is true and correct.

Section 2: The Harris County Judge is authorized to executa, for and on behalf of Harris County, a Request for Waiver, which is incorporated herein by reference and made a part hereof for all intents and purposes as though fully set forth herein word for word.

Section 3: All Harris County officials and employees are authorized to do any and all things necessary or convenient to accomplish the purpose of this Order.

Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of		
Request by Harris County, Texas for	§	PS Docket No. 06-229
Waiver of the Commission's Rules to	§	
Allow the Deployment of a 700 MHz	§	
Interoperable Mobile Public Safety	§	
Broadband Network	§	

WAIVER – EXPEDITED ACTION REQUESTED

REQUEST FOR WAIVER

Pursuant to Section 47 C.F.R. § 1.925(b)(3), Harris County, Texas respectfully submits this Request for Waiver to the Federal Communications Commission ("Commission") to waive any Commission rules that would prohibit Harris County to use the public safety broadband spectrum in the 700 MHz band to deploy a regional, mobile public safety grade broadband data network. Harris County seeks this waiver of the Commission rules to grant design and construction of a fully interoperable, state of the art regional wireless broadband network that is consistent with the Commission and public safety agency requirements, including those noted in the Commission's Waiver grant issued May 12, 2010.[1] Harris County is acting as the principal governmental institution in the East Texas area for coordinating design and build out of this broadband network with the partners as noted and proposed in this document.

Since 1992, Harris County, the third largest county in the nation based on population, has been a leader and driving force behind providing wireless communications for public safety. The Harris County Regional Public Safety Communications System provides interoperable service to 319 agencies from local police, sheriff, EMS, fire agencies, State agencies, and Federal agencies that include FBI,

[1] FCC Order, PS Docket No. 06-229, released May 12, 2010, to 21 Petitioners requesting similar Waivers to the one submitted herein by Harris County.

DEA, ATF and railroad authorities. Harris County has its own staff of installers and project managers, as well as a well trained technical staff for system maintenance and upgrades. The initial system covered Harris County and quickly expanded to provide coverage of the Houston-Galveston Area Council (H-GAC) Region, which encompasses 13 Counties, 12,314 square miles, has approximately 170 miles of Texas Gulf Coastline and serves over 5.866 million in population (approximatiug 24% of entire State of Texas population). The H-GAC 13-county region is deemed by the Federal UASI program to be one of the most vulnerable areas to domestic and foreign terrorism. The Port of Houston, second busiest in the United States and tenth busiest in the world, is one of four in this region (along with Ports of Galveston, Texas City, and Freeport). The area also has an extensive petrochemical industry with a multitude of petrochemical and fuel refineries, biomedical research, nuclear power plant, aerospace (NASA) and major air traffic centers. It further includes the Texas Medical Center, the world's largest concentration of medical research and healthcare institutions.

Harris County has also participated with other public safety agencies and the State in an organization called the Texas Radio Coalition. This Coalition was formed to write the new State Communications Interoperability Plan, which allowed the Statewide public safety agencies to receive monies from the NTIA Public Safety Interoperability Communications Grant. Recently, Harris County partnered with other entities in the eastern portion of the State of Texas to collaborate and expand existing public safety communication infrastructure to cover all or part of 17 additional Counties outside of the H-GAC Region reaching as far north as the City of Longview in Gregg County with continuous coverage south to the Texas Gulf Coast. Harris County along with its partners is positioned to systematically deploy broadband throughout this region as well.

As part of this broadband project there will be a Public Safety Interoperability Gateway (PSIG). It will allow an interface to the large existing Land Mobile Radio (LMR) system, which has over 44,000 public safety users for enhanced interoperability and will create a replicable model for other areas in the State of Texas to follow. The plan is to leverage existing LMR sites along with other county facilities, towers and building

locations for this initial deployment of broadband coverage. The middle mile coverage outside the 13-county H-GAC region will continue north on these LMR sites into Northeast Texas touching all or part of 13 Counties in which the East Texas Medical Center currently provides hospital and medical emergency response. This also encompasses the major evacuation routes leaving the Texas Gulf Coast. The other large partner participating in this collaborative effort is just northwest of Harris County in Brazos and Washington Counties which serves public safety communications for a population of 207,866 and covers 1,194 square miles.

All of these regions cover the entire demographic portfolio of ethnicity, wealth, poverty, urban and rural areas of served and underserved areas. In order to facilitate broadband deployment, the delivery of critical public services in healthcare, education, and public safety and private investment in infrastructure and technology applications for broadband, it is critical that Harris County and the region have a sound and solid middle mile infrastructure. It will enable an expedient, systematic and robust open network to provide broadband to not only community anchor tenants but subsequently to be able to support private, public, and individual connectivity that can then occur through sharing, switching, routing, and governance leadership. This middle mile is essential to last-mile completion of broadband deployment, and will provide a full range of interconnect possibilities to meet provider, carrier, and end-user requirements. Harris County's strategy is designed to foster competition generated by built-in multiple accesses, with the foreseeable reduction in service costs for actual end-users.

Public safety entities in the 28 Counties in the Broadband Interoperability Gateway Network East Texas (BIGNET) area have collaborated to identify community anchor institutions, private entities, and non-governmental agencies to develop a comprehensive, regional public safety network that would provide emergency responders with broadband access and increased interoperability capabilities. Previous regional catastrophic event planning identified key gaps in emergency preparedness and response and underscored the need for a hardened state-of-the-art broadband network that would

be available to emergency responders, not only during routine service but also during a critical incident or a catastrophic event.

The need for such a public safety grade broadband network is particularly acute in the H-GAC area of BIGNET. To address these critical safety needs, the public safety subsystem of the middle mile network that Harris County proposes to deploy will provide public safety and government users with wireless broadband service utilizing 700 MHz public safety broadband spectrum (763 MHz – 768 MHz and 793 MHz – 798 MHz). A subsequent spectrum agreement with the Public Safety Spectrum Trust (PSST) will be based on Long Term Evolution (LTE) standards. The project will enable emergency responders to share information efficiently and quickly and in a cost-effective manner. It will ensure interoperability between system users as well as roaming interoperability with other 700 MHz public safety broadband networks, provide system resiliency and expand access to dynamic multimedia applications. As a result of the BIGNET project, public safety entities will be better equipped to prevent, protect against, respond to, and recover from emergencies.

Public safety and first responders will continue to rely on the mission-critical voicesystem for their essential day-to-day communications and during life-threatening emergencies such as natural and man-made disasters. This voice network will be supplemented by and help support the BIGNET project. Real-time mobile video to and from field officers and "office mobility", (meaning the ability for a public safety official's office to now be "mobile in the field") are two of these applications. Broadband capability is critical during disasters, providing real-time geo-location information about damage, dangers, road conditions, and personnel and vehicle locations. It also allows public safety field personnel to quickly receive data files and video, such as photographs associated with Amber Alerts. In the event of evacuations, like those occurring during Hurricanes Rita and Ike, virtual command centers allow critical systems to be accessed from anywhere, reducing the probability of on-site system failure because of the disaster.

The proposed solution makes it affordable to all entities currently on the existing regional 700/800 MHz system that encompasses much of the eastern one third of the State of Texas. Through partnership with a national public carrier and the use of the PSIG solution, this proposal will allow all system users to roam seamlessly between these areas without concern of losing connectivity. That connectivity's coverage area and potential benefit to public safety is increased dramatically by two other partners in our broadband effort, which are the City of San Antonio and the Texas Department of Public Safety. In our efforts to build this LTE broadband solution the City of San Antonio and State are working closely with Harris County ensure we are able to integrate these projects. The City of San Antonio's FCC waiver has already been approved. Our plan would be for us to leverage our two core switches for redundancy of the core equipment. San Antonio's distance from the Gulf Coast makes it a great location for redundancy. This will create a very robust broadband network with the ability to service all of Texas Public Safety needs. Since the two networks will be connected via major evacuation corridors and across some very rural territory, this partnership will provide robustness to an overall broadband network that will provide the needed redundancy to support the public safety users. This would be difficult to support and undertake alone. Our partnership with the State, the City of San Antonio and others is one reason the state has given us one of the highest public safety ratings on our BTOP application review.

The proposed broadband system will include a roaming agreement(s) with a national public carrier(s) to provide a contiguous connection outside of the BIGNET designated coverage areas. This agreement will provide the offloading of public safety traffic from their network and create a partnership for future broadband initiatives in these regions ultimately benefiting all involved. To address demand and sustainability issues, Harris County, through the selection of the anchor tenants for the build out, designed the broadband deployment strategy to enhance critical services to citizens, which is paramount in building demand for strong broadband service. Identifying these key institutions, which include governmental facilities such as community centers, libraries, public secondary schools, and institutions of higher learning will be important in reaching areas of lower income and underserved sectors of the county.

Euabling Broadband Service In Our Communities

In addition to providing a resilient broadband network for public safety, the BIGNET project can also enable affordable broadband services to the public through Wireless Internet Service Providers (WISP) who can provide broadband Internet access to community anchor institutions as well as business and residential end users. As noted by the Commission in the National Broadband Plan, "broadband is a foundation for economic growth, job creation, global competitiveness and a better way of life." The Commission recognized that ensuring broadband access to community anchor institutions is critical to the operation of this engine. It further noted that improving access to broadband by community anchor institutions "will not only expand broadband options for the institutions themselves but also will improve availability in the community as a whole."

This end of mile solution could utilize unlicensed 5.2, 5.4, and 5.8 GHz spectrum and a broadband Point-to-Multipoint and/or Point-to-Point solution that will enable public broadband Internet access. This public broadband network will be made available to interested WISPs that wish to take part in this Public Access subsystem to further expand the footprint of affordable wireless broadband service throughout Harris, Austin, and Smith Counties by serving community anchor institutions, business and residential end users.

The BIGNET project also will bolster growth in ceonomically distressed areas. As part of the potentiul end of mile solution, Harris County can deploy facilities to which providers can interconnect in order to offer affordable broadband service to unserved areas in Houston. One such area is zip code 77004 which has a 13.3 % unemployment rate and 35.5% of its population living below poverty line (both significantly above the national average). There are a total of 57 zip codes in Harris County, one zip code in Austin County, and four zip codes in Smith County that fall within this criterion. In addition there are a total of 33 zip codes in the three counties with an (average) age of 35 or over that will address the needs of older citizens.

The goal as buildout continues will be to provide this same level of service for critical infrastructure entities, including utilities, pipelines and refineries, along with public access in institutions such as:

1. Healthcare: Houston is the seat of the internationally renowned Texas Medical Center. All 47 member institutions of the Texas Medical Center are non-profit organizations. They provide patient and preventive care, research, education, and local, national, and international community well-being. Employing more than 73,600 people, institutions at the medical center include 13 hospitals and two specialty institutions, two medical schools, four nursing schools, and schools of dentistry, public health, pharmacy, and virtually all health-related careers. The deployment of this initiative will help bridge existing gaps in wireless communications among these facilities and potentially provide public access for patients and other healthcare providers. These same individual entities such as Methodist Hospital are branched out to surrounding counties in the H-GAC region previously discussed.

2. Education: The Harris County Department of Education includes 26 Independent School Districts that have over 1,000 campuses. In additiou, Austin and Smith Counties have 54 campuses that will combine for these three counties to serve as anchor institutions. Higher education of Community Colleges and Universities number 20 campuses, adding to the system's ability to provide broadband capabilities in these areas.

3. Libraries: There will be approximately 37 public libraries that can serve as anchor institutions. These libraries will huve additional access to broadband capability to serve the needs of a community public computing facility. This middle mile will serve to reach the general community during normal business hours and after hours.

Conclusion

Harris County has a proven track record of operating LMR systems, providing mission-critical communications for public safety agencies, as well as other agencies in all levels of government, in the 28 counties of East Texas. We are ready to expand this capability to include a robust, interoperable broadband data network, using the 700 MHz public safety broadband spectrum. The BIGNET project will provide LTE next-generation broadband that will use existing LMR network sites and infrastructure, along with partner public and private facilities. We plan to integrate this broadband network with existing radio network systems to protect approximately one-third of the population of Texas. Such integrated broadband and LMR networks communications will enable public safety to react to any emergency situation in real time by allowing simultaneous radio, video and instant messaging services.

The design of this broadband network will also allow Harris County to work with anchor institutions in the 28-county network to expand services through the collaboration of partnerships with national public carrier(s) and local WISPs to ultimately provide broadband services to the general community in public places and in private homes, using roaming agreements and unlicensed broadband spectrum such as the 5 GHz bands.

In order to move ahead with the implementation of this fully integrated and interoperable broadband network built to meet both public safety requirements as well as eventually the broadband needs of our citizens, Harris County respectfully urges the Commission to expeditiously approve this Waiver Request. This will enable Harris County to proceed with the BIGNET project using the 700 MHz public safety broadband spectrum without further delays. We recognize that the reallocation of the adjacent D Block broadband spectrum to public safety still requires resolution, and we fully support such reallocation by Congress and the Commission. Upon successful Congressional passage of such reallocation legislation by Congress, Harris County plans to expand this waiver request, or file an additional waiver if this request has already been granted, to include the D Block spectrum in this public safety grade broadband network.

Respectfully submitted,

Ed Emmett SC

ED EMMETT
County Judge
Harris County, Texas

Date: August 10, 2010

APPROVED as to Form:
Assistant County Attorney

The Counties that will be participating in the initial build out

Harris County and the following Counties in the H-GAC region:
Austin County
Brazoria County
Chambers County
Colorado County
Fort Bend County
Galveston County
Liberty County
Matagorda County
Montgomery County
Waller County
Walker County
Wharton County

Through Texas A&M the Brazos Council of Government Region Counties that will be participating:
Brazos County
Washington County

Through East Texas Medical Service the following Counties will be participating:
Kaufman County
Henderson County
Upshur County
Panola County
Smith County
Cherokee County
Houston County
Trinity County
Ellis County
Gregg County
Madison County
Leon County
Freestone County

All The counties but Harris County will get a very limited foot print from the initial build out. With the goal of partnering with the carriers for roaming to fill the gaps.

Interoperability Showing Technical and Operational Response

Harris County

Information Technology Center

BIGNET (Broadband Interoperability Gateway Network of East Texas)

Original Date: June 25, 2010

Last Revision Date: August 09, 2010

Table Of Contents

Introduction 3
A. System Architecture 3
A.1 Radio Access Network (RAN) Architecture 3
A.2 Core Network Architecture 4
A.3 Interfaces 6
A.4 Mobility and Handoff (Handover) 6
A.5 Roaming 8
A.6 Priority Access and QoS 10
A.7 Security 11
A.8 Devices 13
B. Applications 14
C. Reliability and Availability 17
D. Radio Frequency (RF) Engineering 19
D.1 Radio Access Network Planning 19
D.2 Interference Coordination 21
E. Testing 23
F. Deployment 25
G. Operations, Administration and Maintenance 28
Appendices 30
Appendix A. Definitions and Acronyms 30
Appendix B. LTE/EPC Functions and Interfaces 32
Appendix C. LTE Test Tools 37
Appendix D. LTE BIGNET Definition & Coverage Maps 40

Introduction

This Interoperability Showing Technical and Operational Response is intended to demonstrate the technical and operational proficiency of Harris County (BIGNET) necessary to achieve operability and interoperability of public safety broadband networks in accordance with FCC Waiver Order 10-79.

A. System Architecture

The Broadband Public Safety solution is based on the 3GPP LTE network solution, and consists of the Radio Access Network (RAN), the Evolved Packet Core (EPC), Devices, and the key interfaces exposed by these components. The solution includes the ability to roam between systems, provide priority access and QoS to ensure the most critical public safety users receive the highest priority, and ensure the Broadband Public Safety solution is secure.

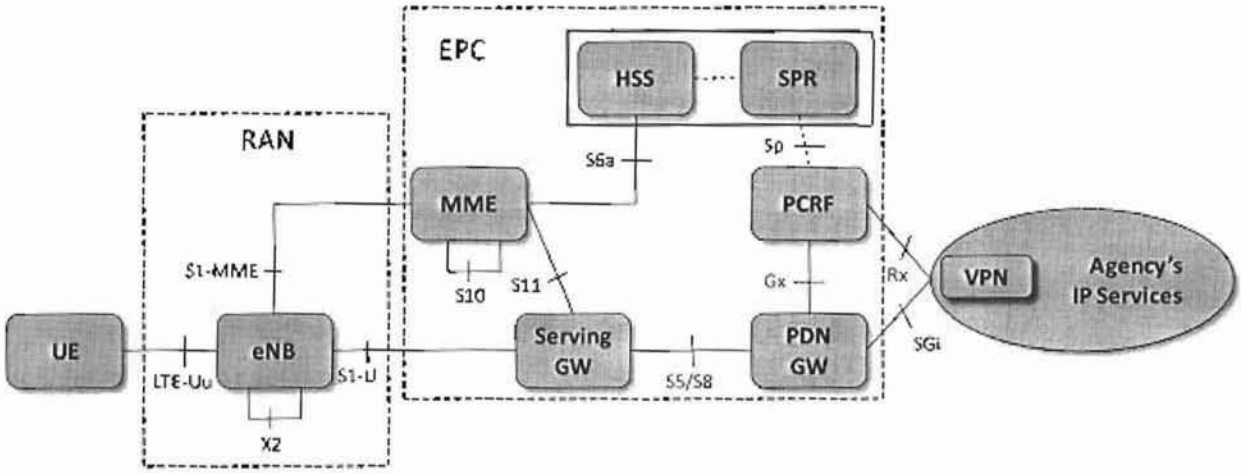

Figure 1 - Logical Architecture

The LTE standard is the right standard for Public Safety broadband use. As with any commercial technology, there are elements in the LTE standard that are not defined based on public safety operations. Issues around inter-PLMN HO support and improvements to access class barring are best dealt with in standards. Issues around priority and pre-emption, especially at the agency, incident or role level are handled by the implementation of this system. Consistent policy enforcement across commercial and regional Public Safety networks requires the correct amount of Public Safety specific standardization that still allows for some regional and agency control.

The LTE RAN and EPC architecture and interfaces are shown in Figure 1 and described in the following sections. A more detailed description of the LTE/EPC infrastructure elements and interfaces is contained in H.Appendix B.

A.1 Radio Access Network (RAN) Architecture

The eNodeB (eNB) is the only 3GPP defined network element within the EUTRAN for 3GPP R8. The eNB provides the user plane and control plane protocol terminations toward the UE. The eNB consists of the inter-working function between the backhaul interface and the base band interface, the base band processing elements for the air interface, and the radios. The eNB in

this system is compliant with the 3GPP R8 standards. The eNB is designed for compatibility with 3GPP compliant UE's and utilizes 3GPP compliant network interfaces.

Functions supported by an eNB are defined mainly in 3GPP TS 36.300. The RAN solution for this system is compliant with the R8 version of 36.211, 36.212, 36.213, 36.214, 36.300, 36.321, 36.322. 36.323, 36.331, 36.413, 36.423 and other referenced specifications. Compliance of devices and the RAN continues to evolve from Dec 2008 to Dec 2009 specification versions and beyond. The eNB is designed to support upgrade to support modifications of the air-interface and network interfaces in accordance with evolution of the LTE standards.

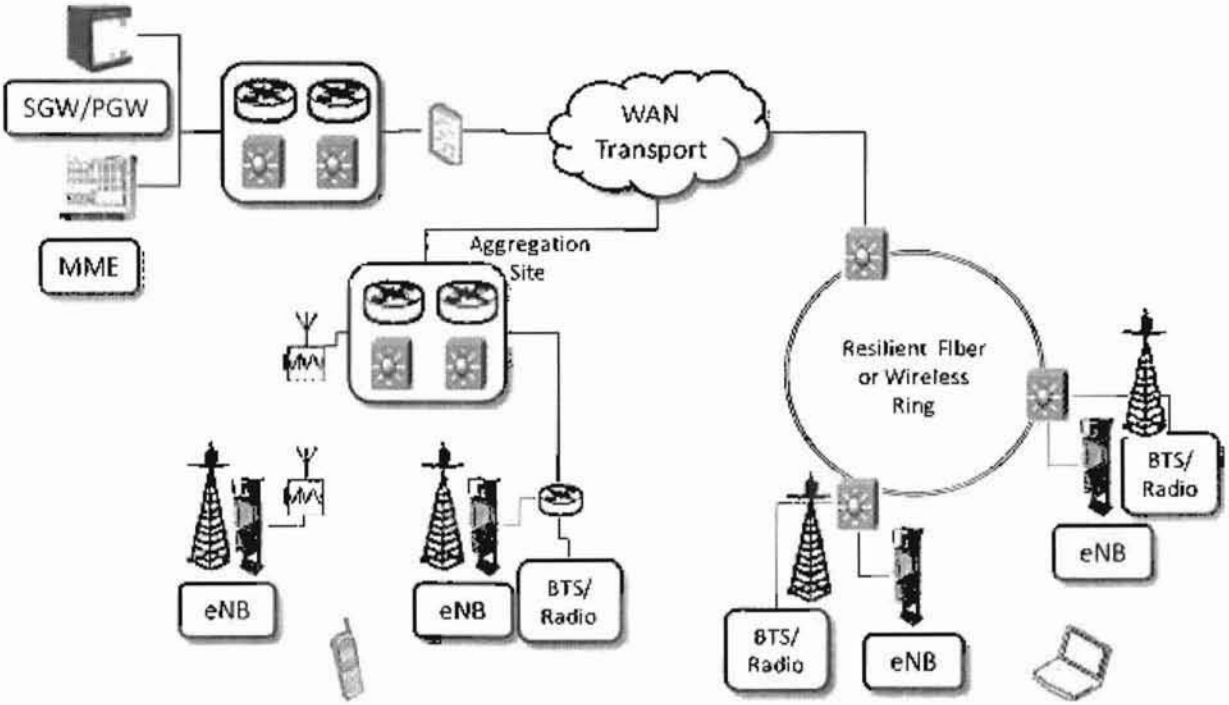

Figure 2 – RAN Physical Architecture

The RAN solution is based on IP transport. The solution supports collocation with existing narrowband or commercial sites and supports shared backhaul of various types. The eNB hardware supports 5+5 MHz PSST band or 10+10 MHz D/PSST band or both D and PSST 5MHz bands simultaneously. The solution will support optical and electrical Ethernet interfaces and can support external L2 or L3 equipment to fit within a number of transport scenarios. Backhaul redundancy is supported when required. The equipment supports the logical User Plane, Control Plane and OAM&P interfaces on the same physical interfaces and supports VLAN separation when required. The eNB is built with Self Organizing Network (SON) functions to automate deployment and optimization functions. The solution will support both GPS and IEEE 1588v2 timing solutions as needed (e.g. for ICIC (Inter-Cell Interference Coordination) or MBMS).

A.2 Core Network Architecture

The core network is based on the 3GPP R8 defined EPC (Evolved Packet Core) as mainly defined in 3GPP TS 23.401. The solution will support the MME, SGW, PGW, HSS and PCRF/SPR functions using standards defined network interfaces. A VPN element is also shown. This element supports a secure public safety VPN and can be used with alternate access technologies (WiFi, 3G).

The EPC solution is based on the GTP-based S5 and S8 interfaces. Support for PMIP-based interfaces is a future roadmap item based on industry demand and will include support for Gxc between the PCRF and SGW. The EPC solution is compliant with the R8 version of 23.203, 23.401, 23.402, 24.301, 29.212. 29.214, 29.272, 29.274, 32.240, 32.251, 32.295 and other referenced specifications. Compliance of devices and infrastructure continues to evolve from Dec 2008 to Dec 2009 specification versions and beyond.

Additional interfaces supporting charging are provided but not shown for simplicity. The PGW and SGW support offline charging interfaces (Gz/Rf/Ga). These interfaces may be valuable in a system supporting multiple agencies and user affiliations.

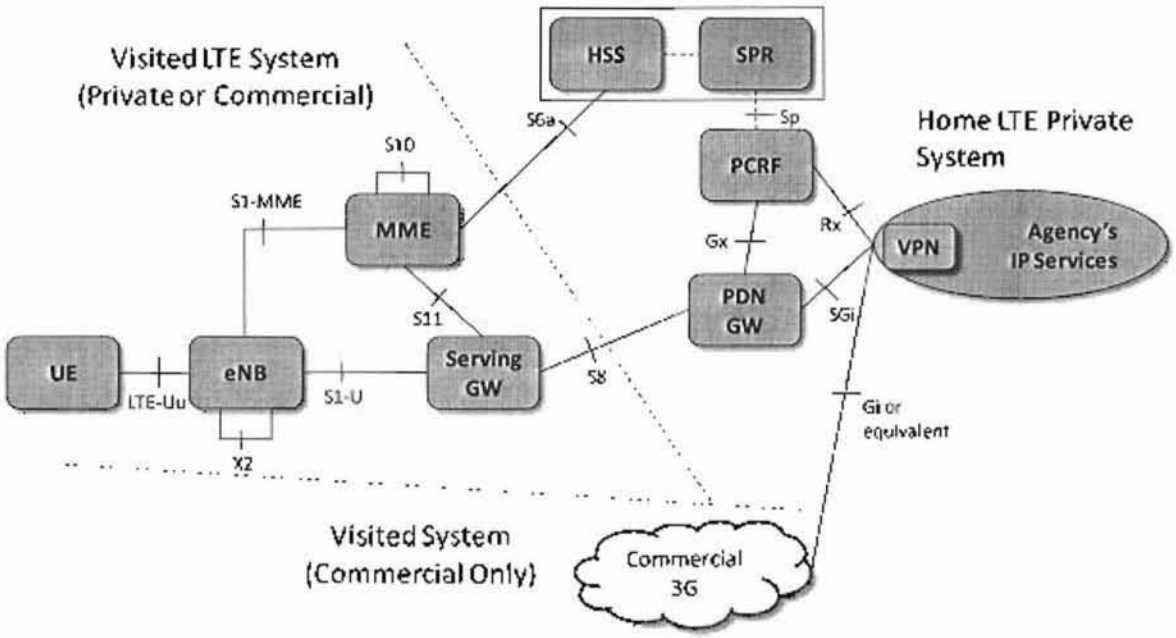

Figure 3 – EPC Roaming Architecture

The system is capable of supporting roaming with other regional PS LTE systems or with a commercial LTE system (if supported by the device capabilities). Note that local breakout is not currently shown (although can be supported). Further study is needed around the impact of supporting a secure VPN and multiple APN's simultaneously. Support for roaming on a commercial 3G network is shown using a VPN solution and a unique subscription on the 3G network. Use of standard EPC interfaces for 3G inter-connectivity between a regional PS network and an existing commercial 3G network run by a different entity are for further study and subject to potential operational complications.

The EPC physical architecture is shown in Figure 4. The EPC solution is based on IP transport and pooling of network elements. The solution supports IPv4 and IPv6 UE's and additional IPv6 network interfaces as a future software upgrade. The solution will support a platform that hosts the SGW and PGW on one platform instance and the PCRF/SPR/HSS functions on another platform instance. Redundancy is supported at several levels including geographical distributed elements to mitigate disaster scenarios.

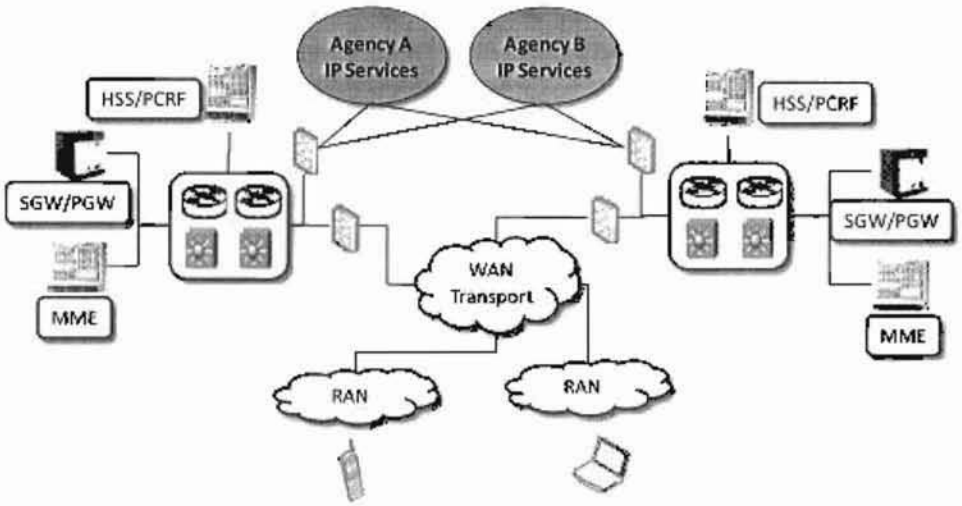

Figure 4 – EPC Physical Architecture

A.3 Interfaces

The RAN/EPC solution will support the following interfaces based on 3GPP R8 compliance:

LTE-Uu, Gx, Gz, Rf/Ga, Rx, S1-MME, S1-U, S5, S6a, S8, S9, S10, S11, SGi, SP, X2.

These interfaces support inter-operability of the LTE network with 3GPP R8 compliant UE devices, as well as inter-operability with other PS regional LTE networks. Details on handoff and mobility inter-operability are addressed in Section A.4 including mobility across regional PS LTE networks. Details on supporting a VPN service are also covered in Section A.4.

A.4 Mobility and Handoff (Handover)

Regional wireless mobile broadband systems, in conjunction with the Shared Wireless Broadband Network (SWBN), present unique mobility requirements, including mobility while maintaining a secure VPN session connection. These requirements are met by leveraging robust and efficient handover algorithms and inter-eNB handover coordination via 3GPP standardized interfaces. The mobility solution accommodates both active and idle mode handovers within LTE networks.

A.4.1 3GPP Compliant Handover

The mobility solution is fully compliant with 3GPP standards. It supports high-speed mobility and seamless handoffs between eNBs within the Broadband Network. Radio frequency phase shift acquisition up to 300 Hz Doppler is supported, which accommodates handoffs above 75 mph in a properly-engineered and functioning network.

The mobility solution will support UE physical layer measurements, as specified in TS 36.214, to determine cell signal strengths and actions specified by the RRC L3 protocol in TS 36.331. The UE receives measurement control information from the eNodeB (eNB) via the following System Information Blocks (SIB):

- SIB3 information block contains common information for both intra-frequency and inter-frequency cell reselection
- SIB4 information block contains neighboring cell related information for intra-frequency cell re-selection including specific re-selection parameters
- SIB5 information block contains neighboring cell related information for inter-frequency cell re-selection including specific re-selection parameters

The MME and eNB utilize UE receiver measurement reports for controlling UE handover behaviors. When making a decision to handover a UE to another cell and/or carrier frequency the following factors or parameters are considered:

- UE measurement reports of its serving and neighbor cell signal strengths
- UE's current signal to interference ratio
- UE's serving cell and neighbor cell loading conditions
- UE's QoS/application profile and the UEs mobility level

A.4.2 Adjacent Network Handover

The mobility solution will support inter-network handover between regional public safety networks. The approach taken to support inter-network handover between regional networks is dependent on several factors. These factors include:

- Frequency bands assigned to and shared between the regional networks
- PLMN ID's assigned to and shared between the regional networks
- Administrative relationships between the regional networks

If the regional networks are allocated a common frequency band, then issues associated with inter-band management are not required. However, if separate frequency bands are allocated to the regional networks, then inter-band handover management functions, such as neighbor band advertisement and frequency selection priority must be supported.

Assuming that regional networks are allocated unique PLMN ID's (see section A.5) then inter-PLMN handover capabilities will be required as regional networks expand and become adjacent. In commercial carrier networks, inter-PLMN handover across operators is not typical. This is because commercial carriers deploy near-ubiquitous coverage in their service areas. Commercial carrier networks may also be comprised of multiple PLMN ID's. However, in these cases, the administrative functions of network planning and operations are managed by the carrier. Thus the carrier is able to coordinate cell identifiers, neighbor lists, and handover configurations across their PLMN ID domains. Since network planning and operations are typically not coordinated across commercial carriers, inter-PLMN handover is typically not supported across commercial carrier networks.

Further, 3GPP R8 standards do not identify the inter-MME S10 interface as a roaming interface. If MME's are deployed in the regional networks (i.e., not shared), then inter-PLMN handover would cross MME domains and the S10 interface would be needed to support inter-PLMN handover across MME domains. Since 3GPP R8 standards do not identify S10 as a roaming interface, inter-PLMN handover across operational domains is not yet supported in the standard. Therefore, in order to support inter-PLMN handover, coordinated network planning and operations across the PLMN ID domains is required. In order to support inter-PLMN handover across operational domains without operational coordination, 3GPP standards enhancements are required.

Similarly, 3GPP R8 specifications do not support LTE<->3G inter-PLMN handover across operational domains. Therefore, handoff across home and visited networks when a visited network is using 3G networks will be gated by availability of 3GPP standards.

A.4.3 Mobile VPN

In addition to handover, the solution also supports Mobile VPN's. MVPN solutions, which are already in wide use by public safety agencies, provide application-level session continuity across disparate radio access networks, as well as security all the way back to the mobile user's home domain. Session continuity is supported at the application IP layer, which is above the radio access layer. Thus, the MVPN solutions can provide session continuity across various

radio access technologies, such as LTE, 3G packet data, and Enterprise WiFi. Each radio access technology comprises an independent link between the MVPN server and the MVPN client in the UE. As such, each radio link is independently monitored and the MVPN selects the optimum radio link to support the application sessions. If a radio link becomes disconnected or impaired, the MVPN can switch to an alternate available radio link. Thus, the MVPN can provide IP layer mobility and intelligent route selection which is independent of handover in the radio access layer. The MVPN can provide an alternative solution to inter-PLMN handover across regional networks, as well as across 3G networks.

In addition to providing IP layer mobility, the MVPN can provide secured connections between the server and client. The secured connection provides authentication, confidentiality, and integrity protection. Cryptographic modules which support the MVPN are compliant with FIPS 140-2 standards. The use of MVPN's with these security capabilities is critical, since current Criminal Justice Information Services (CJIS) security policy requires the use of highly secure VPNs for mobile device access.

A.5 Roaming

Regional wireless mobile broadband systems, in conjunction with the Shared Wireless Broadband Network (SWBN), present unique roaming requirements, including support in initial operations, as well as roaming among regional networks. These requirements are supported by leveraging 3GPP standardized interfaces, as well as adoption of a roaming service tailored to the SWBN.

A.5.1 Terminology and Scope

Using terminology from the NPSTC BBTF report, intra-system roaming refers to roaming across regional networks: "*9.4 Intra-system Roaming - The regional networks will be stand alone systems, part of a single national system, so public safety users roaming from their home regional systems to another regional system are considered to be roaming within (intra) the system.*" Also from the NPSTC BBTF report, inter-system roaming refers to roaming between the national system of regional networks and commercial carrier networks: "*9.5 Inter-system Roaming - Public safety users that are part of a regional system may roam off of the national system and commercial users may roam onto the national system. This roaming is defined as inter-system roaming*"

According to 3GPP standards, home and visited network domains are delineated by PLMN ID. Roaming is the ability for a user to obtain service in a visited network. Note that roaming pertains to obtaining service, whereas handover pertains to the transfer of a user's connection from one eNB or cell to another.

A.5.2 PLMN ID Assignment

The NPSTC BBTF report also recommends that the number of PLMN ID's allocated for the SWBN should be less than 100 IDs, and may be as few as 1 ID. The solution aligns with this recommendation. A unique PLMN ID should be assigned to each region in the US, such as each State or UASI region, and one common virtual PLMN ID should be reserved for the entire SWBN. This scheme allows flexibility and autonomy for regional network operations, yet also provides a single identifier which represents all regional networks in the SWBN.

With a unique PLMN ID assigned to each State or region, roaming as defined in the 3GPP standards will not occur within the regional network. Rather, roaming will occur if a Public Safety user obtains service from a commercial carrier, or obtains service from another regional network. Similarly, mobility within regional networks only requires intra-PLMN (as opposed to

inter-PLMN) handover to support session continuity as users move between eNB's or cells within the regional network. Therefore, mobility within a regional network does not constitute roaming. The solution will support mobility via intra-PLMN handover within regional networks as described in section A.4.

A.5.3 Intra-system Roaming

Intra-system roaming occurs when users obtain service from a visited regional network within the SWBN which is not the user's home network. Intra-system roaming will be supported as needed by operational scenarios which require service across regional network boundaries. Intra-system handover capability can be added as an incremental software upgrade as standards mature. In addition to intra-system roaming, adjacent regional networks will also raise the need for inter-PLMN handover. See section A.4.2 for the solution approach to inter-PLMN handover.

A.5.4 Inter-system Roaming

Inter-system roaming occurs when users obtain service from a commercial carrier network, which is not part of the SWBN. Inter-system roaming will be supported as needed by operational scenarios which cross regional network boundaries, and as allowed by roaming agreements with commercial carriers. As with intra-system handover, inter-system handover can be added as an incremental software upgrade. Inter-system roaming may also require addition of Border Gateway routers to interconnect with a Roaming Service provider. The same 3GPP standards constraints apply to inter-PLMN handover across operational domains for inter-system roaming as for intra-system roaming. However, inter-system and inter-PLMN handover is more challenging due to the additional interfaces and operational dependencies between commercial carrier networks and the SWBN.

A.5.5 Commercial Network Roaming

Commercial carriers typically leverage roaming service providers to provide inter-network connectivity, security, and charging remediation functions. Roaming standards, such as IPX, are evolving to support QoS-enabled IP transport services, and therefore should support the services required for roaming with commercial carriers. However, inter-system roaming may have unique requirements as compared to commercial carrier roaming services, such as the support for the large number of regional network entities comprising the SWBN. Therefore, it will be beneficial to establish an SWBN roaming service to minimally support intra-system roaming. In order to support inter-system roaming, the SWBN roaming service could then interface to commercial roaming service providers, representing a single point-of-presence for the SWBN.

A.5.6 Roaming Interoperability

UE's conforming to 3GPP standards will be able to roam across regionally deployed networks. However, it is essential for the UEs to be configured with appropriate frequency bands, PLMN lists, and access parameters corresponding to associated roaming agreements. 3GPP compliant UE's will minimally support the following roaming-related behaviors:

- Scan supported/configured bands,
- Perform network and cell selection,
- Authenticate on a visited network.

After authentication on a visited network, an IP address is assigned, and the UE then has the ability to access IP services. If home routed session is initiated, then the home network assigns an associated IP address to the UE. If a local breakout session is initiated, then the visited network assigns an associated IP address to the UE.

A.5.7 Roaming Configurations

The solution will support home routed roaming configuration. Home routed configuration is when a user's traffic is routed back to the home network to enable the use of home applications and Internet access. The home routed case can support the majority of Public Safety applications and use cases. Home routed bearer flows benefit from QoS policies controlled in the home network. In addition, home routed provides many operational and security benefits, such as:

- Single point of authentication for applications
- Single point for firewall, intrusion detection/prevention, and anti-virus protection
- Activity logging and Internet access policy control

The solution will also support local breakout roaming configuration as needed for Public Safety applications. Local breakout configuration is when a user's traffic is routed within the visited network, and therefore is not routed back to the user's home network. Local breakout provides for optimization of bearer routing and access to visited network services. It should be noted that roamers may be subject to QoS policies of the local (i.e., visited) network. This is because 3GPP R8 standards allow the visited network to overrida QoS parameters from the home network. For this reason, the local services provided in the visited network are likely to be limited to IP services with static QoS and priority (e.g., best effort) for roaming users. It should be noted that the S9 interface is only applicable to local breakout scenarios. The S9 interface is used to provide dynamic charging and QoS policies from the home network to the visited network. Since use of local breakout scenarios are expected to be limited to static QoS policy, use of the S9 interface may not be required to support Public Safety applications. See section B for additional information regarding configurations used to support Public Safaty applications.

A.6 Priority Access and QoS

LTE offers the most advanced QoS capabilities of any commercial cellular technology; however the technology must be properly configured for optimal public safety implementation and to support roaming (with carriers and other public safety regional systems). This section provides an overview of tha solution while highlighting tha interoperability configurations for public safety. These LTE configurations should be standardized across all public safety regional systems in order to facilitate nationwide interoperability. The system defined in this section is compliant with 3GPP TS 23.203.

A flexibla priority access and QoS framework is provided by the solution:

- **Regional Flexibility**
  Each public safety region has the flexibility to choose an LTE prioritization model to suit its need. For example, region 1 may prioritize responders based on role and region 2 may prioritize responders basad on application. The region should have some latitude to choose how to prioritize devices and applications on the regional system.

- **Roaming Support**
  Whether roaming between ragional systems or roaming to a commercial LTE system, the prioritization framework can support a consistent and fair policy of mapping priority betwaen systems.

The realization of this framework is standardization of LTE configuration parameters for public safety use, such as ARP, QCI, GBR, and MBR. H.Appendix C lists the specific LTE system configuration necassary to achieve interoperable priority and QoS between two systems that are involvad when roaming is utilized. The reader will appreciate that these recommendations must

be consistently applied to all 700MHz commercial and public safety LTE systems in order to achieve meaningful interoperability.

A.7 Security

Security is a critical aspect of the public safety broadband network solution. This section describes the comprehensive and interoperable security solution included in the offering.

Overall security architecture

3GPP standards have defined a suite of security related specifications for LTE systems. The 33 series of 3GPP specifications contains several documents defining various aspects of LTE end broadband application security architectures. From an interoperability perspective, of particular interest are the specifications 33.401 ("3GPP System Architecture Evolution (SAE); Security architecture"), 33.210 ("3G security; Network Domain Security (NDS); IP network layer security"), and 33.310 ("Network Domain Security/Authentication Framework (NDS/AF)"). The solution will fully support the requirements stated in these specifications to ensure secure inter-system interoperability.

The solution will support both the mandatory and certain optional aspects of the 3GPP SAE security architecture specification, as defined in 33.401. The optional aspects the solution considers mandatory align with recommendations given by the NPSTC Broadband Task Force. Specifically:

- Both control plane and bearer plane traffic will be encrypted over-the-air. This includes RRC signaling, NAS signaling, and user plane traffic.
- 33.401 requires the support of both the SNOW 3G and AES encryption algorithms. AES will be default choice in the solution, since it is a NIST/FIPS recommended algorithm for securing public safety communications.

The solution will utilize secure O&M protocols and methods to distribute software and configuration information to the network elements.

Network Domain Security

The solution will implement the 3GPP defined mechanisms for Network Domain Security, as defined in the 3GPP spec 33.210, "Network Domain Security, IP Network Layer Security". Per 33.210, the interfaces between the network entities in the network are to be secured using IPsec security associations. The security associations will be established and maintained using either IKE (Internet Key Exchange)v1 or IKEv2. Per 33.210, the Ze interface is used to interface between two security domains and the Zb interface is used to interface between the various network entities within a single security domain. Specifically:

- NDS/IP inter-domain interface (Za) cryptographic protection via Security Gateways (SEGs) will be provided. The Za interface security associations will be established using IKEv1 or IKEv2. X.509 digital certificate based authentication will be utilized between SEGs in different security domains.
- NDS/IP intra-domain interfaces (Zb) as specified in 33.210 will be cryptographically protected unless within physically secure and/or fully trusted environments.

Inter-Domain Trust Establishment

In order to facilitate interoperability for establishment of trust across potentially large numbers of public safety security domains, a scalable mechanism is needed for establishing security associations, whether at the network domain level or applications/services level. Digital certificates and Public Key Infrastructure (PKI) based trust management are the methods defined in 3GPP specification 33.310 for achieving these goals.

The solution supports the methods defined in 33.310 for creating, exchanging, and validating digital certificates across security domains. These mechanisms ensure that regional broadband networks have policies and protocols in place to establish a basic, interoperable authentication framework. As discussed in 33.310, the selection and design of the appropriate PKI based trust models will need to be made (e.g. the use of cross-signed certificates between the security domains vs. the use of a trust bridge model via Bridge CAs). In addition, work will be needed to define public safety specific certificate policies that further enable interoperability.

Coordinated certificate policies can help interoperability by defining common rules for the usage of digital certificates in a system. Some examples of policy parameters that are important to interoperability include:

- consistent rules on certificate issuance vetting and authentication
- agreed upon methods of safeguarding Certificate Authorities
- personnel security controls
- selection of public key crypto key sizes and algorithms

By having such policy elements consistent across systems, the difficult task of policy mapping between security domains can be minimized.

MVPN Access to Home

The Waiver requirements specify that petitioners' systems allow the use of network layer MVPN access to any authorized site and to home networks on the deployed network. This requirement is designed to ensure the ability of first responders to securely connect back to their home systems when attaching to foreign wireless networks. Without this requirement, there is the risk some deployments may have their wireless networks configured to discard any traffic that is encrypted and destined to an external domain. This would be very problematic, as there are security compliance policies by CJIS, and NCIC (National Crime Information Center) that require the use of VPNs for remote user access.

CJIS (Criminal Justice Information System) requirements mandate the use of FIPS 140-2 validated encryption. Thus any user of a deployment utilizing a broadband waiver must use FIPS 140 validated solutions to be compliant with CJIS security policy and to access CJIS related services. The solution will use FIPS 140-2 compliant MVPN solutions for remote user access.

Application Security

Application security is first provided by limiting access to authenticated users through the use of MVPN access to the home system. Once access has been authorized and secured, user authentication to specific applications such as the local status page will be required per local policy.

The specific authentication framework has not been specified by 3GPP or PSCR. The following represent the desired capabilities of the application authentication method ultimately selected.

- The security framework should provide authentication and authorization information between security domains (e.g. between Waiver Recipients)
- The security framework should provide single sign-on solutions that are compatible with existing commercial web browser user agents.

The use of a federated identity management solution enables portability of identity information across different agencies. This is essential to enabling many application security interoperability use cases. The creation of such a federated identity management solution is a work in progress. As such, the final solution should be specified with input from the public safety and