NIST Nationwide Public Safety Broadband Network Comments

We are pleased to respond to NIST's request for information regarding the proposed National Public Safety Broadband Network (hereafter referred to as the 'NPSBN'). ESD America believes that the NPSBN represents an opportunity to revisit old paradigms of delivery for the needed information for public safety team members. The requirements listed cannot be met by a network solution alone, and we believe that we can provide benefit both with a prototype hardware platform, as well as considerable experience delivering secure communications in challenging communications environments. We are happy to partner with other providers who can provide the needed network capability on the newly available spectrum, but also believe our solution can allow certain key requirements of the NPSBN to be field-tested before the new network is ready, as well as provide a platform ready on current networks for voice, data, video and applications development on a ruggedized, capable device. Below is a brief response to the NPSBN proposal, which was obtained at http://www.gpo.gov/fdsys/pkg/FR-2011-09-12/pdf/2011-23180.pdf.

ESD America and GSMK Cryptophone Capability

The ESD America is proud to present the GSMK Cryptophone suite of products as a capability key to delivering on a number of the proposed requirements. The GSMK Cryptophone software has been deployed on a number of Windows Mobile compatible handsets, providing a hardened operating system, FIPS 140 verified cryptosystem, secure voice, secure text, and secure file storage as key capabilities over GSM, 3G, Satellite, fixed-line and wireless network environments. The current platform is IP-based, and is proven to operate in challenging network environments with very low latency, high call quality, and very high security. The platform is also ideal for the development of varied application platforms, and can utilize a range of accessories. There is simply no better platform for interoperable, secure voice and text solutions available on the market today.

The items specifically able to be handled by the ESD America with the GSMK Cryptophone products are listed below:

Req. 2. At a minimum, access to initial and updated basic incident information (voice- and text-based incident data);
Req. 3. An infrastructure that is hardened and secure, providing a high level of system availability;
Req. 4. When voice is converged for normal operations and in the event the infrastructure is compromised, public safety communications must remain stable and with clear voice communications;
Req. 5. Geographic coverage that has no limitations within the footprint of the National Public Safety Broadband Network;
Req. 7. Interoperability, including with existing public safety-based systems;
Req. 10. Single devices that support voice, video, and data;
Req. 11. Access to and from external information sources;
Req. 12. Easy integration with other technologies;
Req. 14. Current and future enhancements available to commercial consumers are provided to public safety with no limitations; and
Req. 15. Ability to send, receive, and process information from the public (citizens and media).

In the further, more detailed response we have generalized the above items into three key components:

- Network Availability
- Single Device Capability
- Security
- Interoperability and Extensibility

General Comments

ESD America would like to comment on the requirements detailed, and provide an opinion on the overall intent and purpose of the process.

The nominated requirements cannot be met with a new network alone, and will require a set of equipment and software that currently exists, but is not being utilised to its full potential. In fact, the majority of the benefits of the NPSBN could be obtained today with existing products, and allow for in-field testing of the core concepts of the NPSBN before the network is selected and deployed.

Without an open network infrastructure however, the benefits of interoperability, access to information, use of commodity hardware, and ability to scale in a cost efficient manner will not be obtained. Consider the difficulties of the current secure mobile radio technology, and the difficulty of operating on, and integrating with SIPRNET as examples of the significant obstacles to overcome if implementing non-standardised networks. Developing security models on a per-application and per-agency basis is dynamic enough to allow for integration, without otherwise stifling the ability to cooperate and coordinate between agencies and teams in the event of an emergency.

ESD America's position is that existing products by ESD America can provide secure voice and text services, and allow access to secure data services such as the world wide wide and email as required over VPN or SSL services. The products can run on all IP based networks including transit over satellite, GSM, WLAN and Bluetooth PAN, allowing extremely flexible deployment scenarios, and flexibility for the end user in the event core services are not available. It has already been tested on proposed emergency private mobile networks for military and government, and is ready for field deployment now. In fact, if access to the NPSBN was available using an equivalent to current 3G 'hotspot' devices, virtually all of the current requirements could be met by the GSMK Cryptophone, without requiring the purchase of any new end-user equipment.

Network Availability

Using a combination of access to multiple networks, such as Satellite, GSM and Wireless will allow the GSMK Cryptophones to act as components in a multi-technology highly fault-tolerant network. The nature of the device means it natively accesses typical consumer networks, which also allows the ability for the devices to use consumer networks where more cost-effective, or where deployment of application services on consumer networks is more effective.

GSMK technology for securing voice solutions will allow security of the voice communications, whilst still providing excellent audio quality, low bitrates, low latency and capability to elegantly handle unstable network conditions.

Integration of mobile networks such as is possible with the GSMK Cryptophone can also alleviate issues with integration of non-critical staff, or ad-hoc teams of emergency responders, as the devices are suitable for everyday use while still capable of operating in a secure fashion.

Also the integration of a device capable of operating using Satellite and mobile signals completely removes any geographic limitations for responders, and allows access from high altitudes, something difficult to obtain using terrestrial communications systems.

The GSMK Cryptophone platform is flexible enough to operate on virtually any IP-based network and over Carrier Switched Data (the original Cryptophone platform). It can also operate on public or private servers, allowing flexible deployment and deployment on ad-hoc emergency networks if required. The data-based model also means that there is little limitation with the number of simultaneous calls, unlike traditional call environments that can be easily overloaded in emergency situations. The data-based model also provides easy QoS implementations, allows better filtering/prioritisation of Public Safety data in the event of emergency, and removes dependencies on voice switching infrastructure – meaning data can be prioritised over voice, providing additional benefits when more critical services are data-laden.

It is also worthwhile to note that the ability to transfer voice over data links is extremely difficult to execute, particularly when combined with encryption, and potential low-bandwidth or low-reliability networks, such as may be the case in disaster scenarios. The GSMK Cryptophone Voice codecs and implementation is proven over high latency environments, and yet still extremely efficient and fault tolerant – and can be demonstrated now, allowing rapid achievement of key NIST goals.

Single Device Capability

The current ESD America flagship model, the GSMK CP450, is a rugged mobile phone that admirably meets the 'Single device that supports voice, video, data' paradigm. It allows transfer of all of the nominated data sources, as well as having in-built camera, GPS module and fingerprint scanner. ESD America has partnered with Motorola to allow continued development of this platform, and enhanced integration between hardware and software.

A second prototype has already been tested on the existing Terrestar Genus platform. This platform provides an integrated Satellite and mobile network platform, on a single device.

Other GSMK models are customised from standard commodity phones, allowing for accessories such as GPS, accelerometers and full Bluetooth connectivity as standard.

Unlike some other mobile operating systems, Windows Mobile is not hampered by restrictions on the OS, carrier or handset manufacturer, and allows considerable extra freedom for application developers to coordinate and share data, and obtain 'bare-metal' access to subsystems such as Bluetooth and GPS, providing the ability to obtain high-accuracy GPS fixes for example.

The end result is an ideal platform for consolidation of capabilities to a single device, or as a 'hub' device capable of integrating multiple sensors, networks or data systems into a single view for the end user.

Security

The GSMK Cryptophone system meets the needs of the varied user base of the NPSBN by being built on a Common Criteria verified, yet still commodity operating system, and providing FIPS-140 compliant cryptosystems for the encryption of voice, SMS and local filesystem data.

Using the GSMK IP-based secure voice system will also allow an additional level of verification of access to the voice environment, by requiring registration of the handsets to the IP server. Private Servers can be deployed for specific user groups, and can be deployed on private networks if required, such as emergency mobile networks. This helps to provide the Strong, Dynamic Access Control goal, at least for voice and text services over the network. Due to the once-only nature of keys, revocation of a users access will not affect any other users, and compromise of devices does not compromise the security of previous or future conversations, unlike competing solutions in the mobile and secure radio arenas. The same criteria can also be met on standard data links by extending the authentication mechanisms of network-based applications and services to operate in a similar fashion.

Applications with individual security requirements can be handled using the Operating System controls, and by using specific application 'white lists' which can be generated for the system if required.

Windows Mobile also provides full support for SSL in FIPS compliant mode, and the opportunity to connect to a variety of VPNs.

Windows Mobile provides sophisticated management capabilities that can be configured as required for a customer to configure the device for remote wipe, application of security profiles, and other features as supported by the ActiveSync protocol.

Interoperability and Extensibility

The GSMK secure voice system also works over commercial networks, satellite, private networks, and already operates over Bluetooth and Wifi. It provides a mechanism for apps and widgets to be deployed, uses the existing HTC and Motorola accessories, and OS upgrades are easily deployed when available, but for security reasons cannot be deployed 'Over the Air'.

Usage of the Windows Mobile 6.5 platform allows easier development of single-purpose applications for specific purposes, able to integrate together, and avoiding the need to deal with cumbersome methods for inter-application communication like most competing mobile platforms.

The ability to deploy secure voice, including use of teleconferencing facilities to allow the infrastructureless secure voice over Carrier Switched Data or even ad-hoc wireless networks, and the same capability when using text systems is available now, as is multi-party secure calls using the IP-based solution and teleconferencing units.

The GSMK Cryptophone, being able to operate on public networks, can be easily deployed to various user groups such as individual police or fire units, or public safety organisations immediately, and without costly customisation or configuration.

This makes it perfect for small implementations, and being future ready for the public safety network, providing it is IP-based, makes it a perfect complement to the NIST goals.

The GSMK Cryptophone would also be an excellent candidate for a testbed/prototyping/research platform, offering larger customisation options than many competing handset manufacturers and operating systems.

Additional Device-Specific Requirements

ESD America provide a range of secure, mobile, interoperable devices that operate over a range of network protocols, and provide needed secure communications in challenging and adverse environments.

Because of this experience, we can demonstrate that most of the NIST requirements can be met using existing technology, and if using a variety of networks, can provide the needed coverage and feature set immediately, allowing proof-of-concept application and deployment scenarios to be tested before the full roll-out of the NPSBN.

It is for this reason ESD America considers the development of key interoperability and end-user device capabilities critical to the development of an environment that meets the needs of NIST and the US Government as a whole. This should include, as a minimum:

- Requirement that end-user devices be agency configurable
- End-user devices should support government mandates for encryption and device configuration, e.g. FIPS-140 and Common Criteria
- End-user devices should operate on the NPSBN, and at least one commercial network
- End-user devices should, as a minimum, have full GPS connectivity (ideally providing NMEA or similar device-independent data format) and full Bluetooth stack, allowing the connection of serial, data, media and networking devices.
- Devices should be capable of being operated by gloved hands, except where specifically excluded, such as specific tablet PCs.
- Devices should be capable of operating on standard IP networks
- Devices should provide the capability to defend themselves from attack, such as implementation of anti-virus and/or firewall capabilities.
- Devices should be capable of encrypting local data storage to prevent compromise in the event the device is lost.
- Encryption keys on a device must be capable of revocation
- All data encryption keys, such as SSL, voice, etc. should in preference, be generated at the time of use and discarded after use to prevent post-event communications compromise.

Summary

The GSMK solution can provide a number of unique benefits is a way that plugs many of the gaps in the ability to provide the Nationwide Public Safety Broadband Network on existing commodity systems and hardware. As mentioned above, the solution is ready now, and can be used as a model and for research during the development and phased deployment of the NPSBN. Many of the key features could be realised now, providing quicker return on investment, and better capabilities to public safety organisations. The ESD America is happy to work with consortia on development of additional interaoperability and device requirements, advice on a full end-to-end comprehensive solution, and to provide displays of functionality on the existing demonstration network if desired.

If you have any further questions about this response, or for commercial discussions, please contact Les Goldsmith

(contact details here)