Direction Finding Abducted Children: Proposal For A New Amateur Radio Emergency Service

Brian Neill – VA3BPN

July 26, 2003

Abstract

This paper is a proposal for a system that would enable amateur radio operators to pinpoint the location of an abducted child. Where possible the system uses equipment and protocol that is pervasive throughout the amateur radio community such as 2-m equipment, digital communications, direction finding equipment, APRS and ham emergency preparedness.

This system does require that the abducted child be carrying a special device. While this paper does not provide specifications for the actual device, a set of functional requirements are proposed in the hope that some qualified amateur will attempt to prototype and build a child location device (CLD).

Parent's and children's privacy are given due consideration throughout this paper. A number of security controls and mechanisms are included to ensure that police are the only party that is able to activate a child's device; and they must obtain key information from the parent before they are able to activate. The security controls aim to reduce the possibility of abuse, protecting the system and ultimately the child carrying a device (CLD).

Finally, the appendix suggests an operations framework to be used in a DF enabled search for an abducted child. This framework example is provided, as a means to describe how the ham community can respond to this class of emergency, should police ask their local amateur radio club for assistance.

Table of Contents

Table of Figures

1 Motivation

In May 2003, a 10-year-old girl named Holly Jones was abducted from her neighborhood in the west end of Toronto, Ontario. Holly had been walking home from a friend's house at the time. 24 hours later her dismembered body was found off the shores of Toronto Island in Lake Ontario.

Police need tools to aid them in quickly finding children who have been abducted. The amber alert system is one such tool meant to quickly distribute information, critical to saving a life, to the public. This system is an excellent example of how police can work with media and the general public in times of emergency.

Volunteering effort and expertise during an emergency is a familiar idea to amateur radio operators. We pride ourselves on our readiness and availability in the event of an emergency where communications equipment and qualified operators are required in short order.

What if we had the means to find an abducted child, using equipment that is pervasive to our hobby? Amateur radio operators are everywhere, and police would have an immediate and influential tool at their disposal.

This paper aims to pull existing pieces of our hobby together, proposing a system that would enable amateurs to search for an abducted child.

2 Overview

This proposal is intended to outline components and procedures for a new amateur radio emergency service that will allow Hams in conjunction with Police to conduct Direction Finding (DF) search operations for missing or abducted children.

DF gained infamy during WWII's Battle for the Atlantic, where Allied aircraft would be dispatched to sink enemy German U-Boats that had been pin-pointed by Allied radio listening stations. When a U-Boat used his radio to transmit, the land based listening stations could infer a position.

The concept of Direction Finding is that a transmitter's signal is strongest when a receiver uses a directional antenna and points it in a straight line to the transmitter. This produces a vector and when three or more receivers participate, the resulting vectors can be drawn on a map, the transmitter is located at the point of intersection.

In practice the concept is more difficult, however, some ham operators have made a sport out of hunting transmitters using this method, called "fox hunting".

This paper proposes using DF techniques to track down missing children that are carrying a Child Locator Device (CLD). Although the device (CLD) is not specified here, a set of requirements are listed in the hopes that some capable amateur will further develop the device (CLD) in the future.

The device (CLD) is not simply a transmitter, it must be intelligent enough to guard the privacy of the child so that only police, working with the consent of a parent, can activate the device and locate the child. For this reason the device (CLD) must have a digital receive capability as well as a computing capacity to process a Police generated activation code.

The activation code is generated with state of the art, public key cryptography, a technology that has had little value in amateur radio, since codes and ciphers are not allowed on amateur bands. As described below, these cryptographic mechanisms are employed to ensure authenticity, not secrecy, and are therefore a viable control to be used over the air.

Finally, a procedural framework for a DF enabled search is outlined in the appendix. One of the fundamental concepts of our hobby is that we as amateurs will use our technical expertise and resources in the service of our community, especially during an emergency. A child gone missing is an emergency.

3 Requirements for Child Locator Device

Requirement	Description
3.1	CLD must be self contained with an integrated antenna, power supply, receiver, transmitter, and any required processing hardware.
3.2	CLD must be able to receive and process a digital signal from a standardized (static) amateur frequency.
3.2.1	The CLD should receive a signal over 2m generated by a TNC.
3.2.2	The CLD should receive a DSS (Digital Spread Spectrum) signal over a designated amateur microwave frequency.
3.3	The CLD will implement a state-machine with 2 states. Transmit-inactive and transmit-active.
3.3.1	The CLD will start in transmit-inactive and will move into transmit-active only upon receiving and verifying a valid activation code.
3.3.2	When the CLD is in transmit-inactive state, it will never transmit.

3.4	When the CLD is in transmit-active state, it will transmit a continuous audible tone (beacon) on a designated amateur frequency on 2m (DBF) using FM.
3.4.1	The CLD will continuously beacon on the DBF until it loses power.
3.4.2	The CLD should operate in a reduced transmit capacity when it is low on power.
3.5	The CLD must be capable of producing a beacon for at least 2 hours.
3.6	The CLD must be capable of transmitting a beacon that can be received at a range of 1 kilometer.
3.7	Activation Codes with a serial number that does not match the CLD's serial number must be ignored.

Requirements 3.2.1 and 3.2.2 are mutually exclusive; 3.2.1 capitalizes on the pervasiveness of mobile APRS equipment within the ham community, where 3.2.2 aims to reduce cost and size of the device (CLD) by possibly using modified components from the cellular telecommunications industry.

4 Protecting Children's Privacy

Privacy is a prominent concern of any system that can be used to track an individual, especially a child. How does one prevent a potential abductor from using the device to locate a child? What prevents the unintended use of the system by police? Can the security of the system be broken?

To answer the latter, a system can never be 100% secure. However, the mechanisms described below purposely protect a child against unauthorized and unsolicited activation of devices (CLDs).

In order for a device (CLD) to start transmitting it must receive a valid activation code over the air. An activation code is a combination of a device serial number and a digital signature where the digital signature portion of the activation code can only be generated using a cryptographic private key to 'sign' the device's serial number. There are actually two keys involved in this process: a private and a public key. The private key is used to 'sign' and is intended to remain a secret, where the public key is used to 'verify' a signature and can be widely distributed. The public key is embedded in every device CLD, and in order for the activation code to be accepted, the CLD must be able to 'verify' the signature portion of the activation code using the public key.

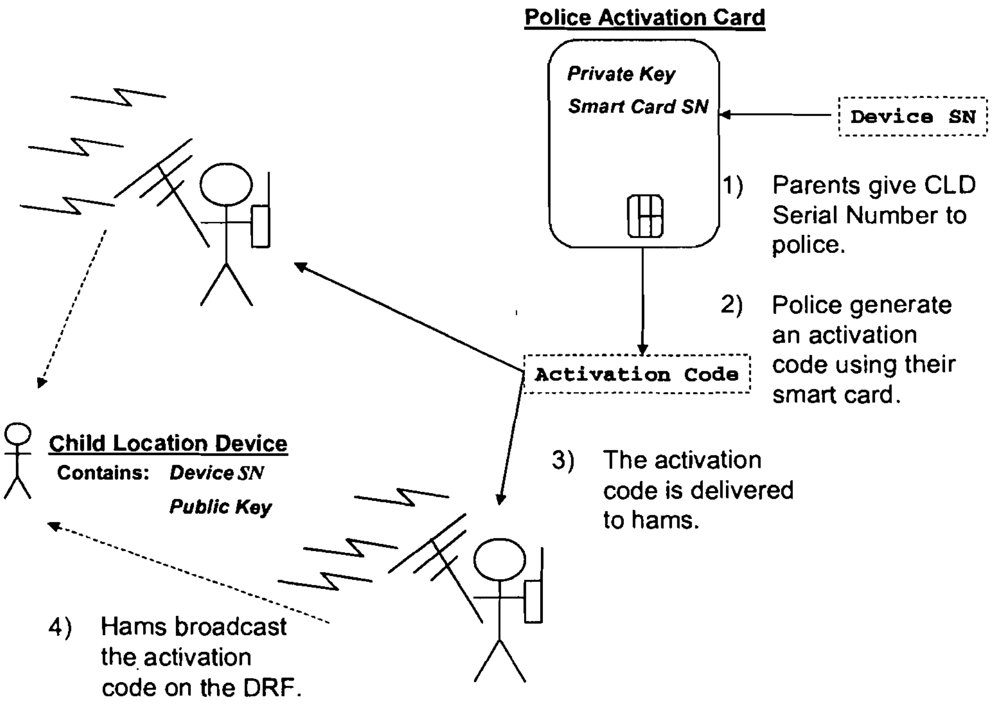

Police Activation Card
Private Key
Smart Card SN
Device SN
1) Parents give CLD Serial Number to police.
2) Police generate an activation code using their smart card.
Activation Code
3) The activation code is delivered to hams.
Child Location Device
Contains: Device SN
Public Key
4) Hams broadcast the activation code on the DRF.

Figure 4-1 : Activating the Child's Device

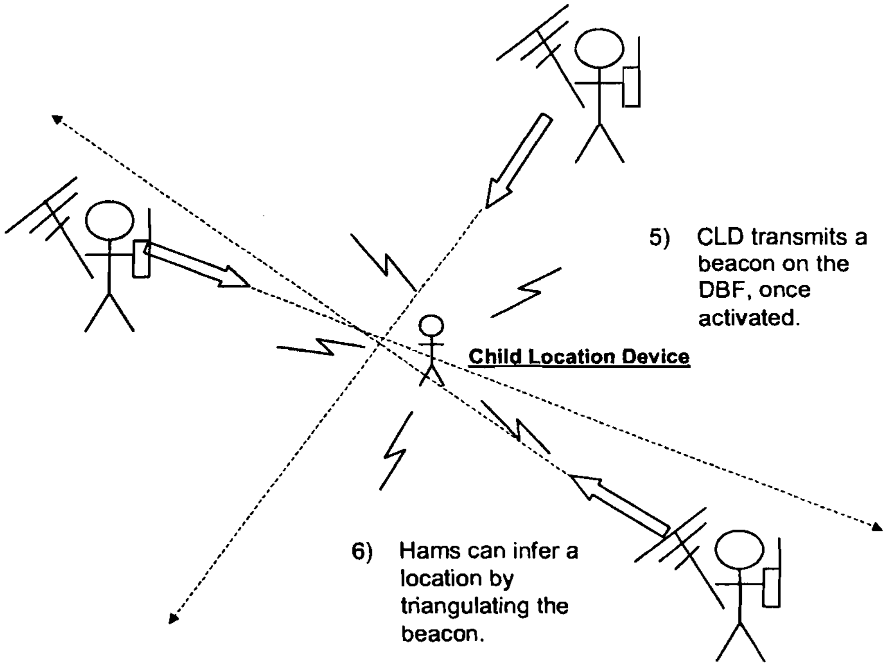

5) CLD transmits a beacon on the DBF, once activated.
Child Location Device
6) Hams can infer a location by triangulating the beacon.

Figure 4-2 : Locating a Child

Guessing the value of the digital signature or the private key is considered an intractable problem. In other words, it would take decades of trial and error[1], without the private key, to produce a valid activation code for a particular device (CLD). Of course, given the nature of computers and Moore's Law[2], computers are becoming faster and more capable of solving large mathematical problems. To contend with this issue the system uses a key size (4096bit RSA equivalent strength) that is expected to be "hard to solve" for the next 10-15 years. By choosing a strong key, and keeping access to this piece of data restricted and tightly controlled, devices (CLDs) are afforded a high degree of protection well into the next decade.

The "protection", however, is only mathematically speaking since there are other ways an attacker can compromise the system. The most effective low-tech attack would be to steal the private key. This poses a dilemma, how does one distribute the private key to any number of police agencies while containing the risk that the key may be accidentally or maliciously exposed? The key must be available to police so they can initiate a legitimate search for a missing child, however, it must also be protected against theft and abuse.

To solve this dilemma, the key will be stored and secured on a limited use smart card. A smart card is small computer chip (without a power supply) that is embedded in a piece of plastic that looks like a credit card, and the concept behind the technology is that one can store a cryptographic key and perform cryptographic operations directly on the card. Physically trying to "open" the card to remove the chip and learn the key irreparably damages the card and it's data before any useful information is discovered.

[1] Using a massive amount of computing resources. For an example of the computer power required to guess private keys see http://www.certicom.com/about/pr/02/021106_ecc_winner.html Note: An ECC private Key utilizing a 109bit curve is roughly comparable to a 512bit RSA key. ECC 163-bit ≅ 1024bit RSA. This system proposes using keys equivalent to 4096bit RSA.

[2] Moore's Law states that the number of transistors per square inch on integrated circuits doubles every 18 months, effectively doubling the availability of "affordable" processing power.

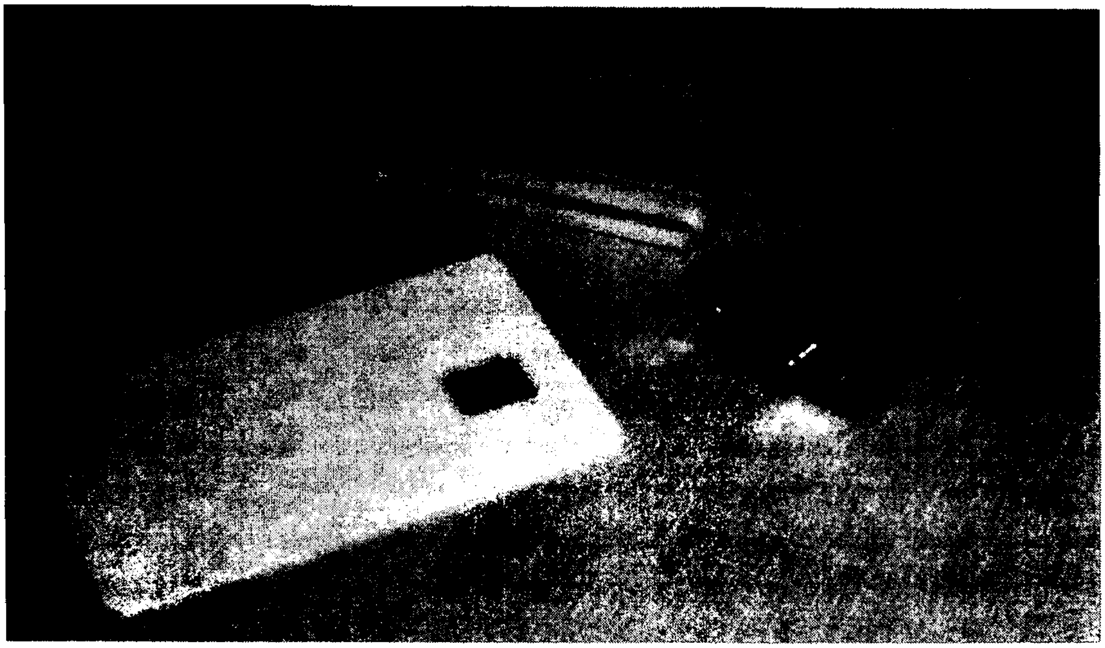


Figure 4-3 : Picture of a Schlumberger JavaCard & Smart Card Terminal

Schlumberger manufactures the smart card featured in the figure above, it retails for approximately $20 US per card and its defining feature is that it allows custom programs to be loaded and run on the card. A card similar to this one would be used to sign device serial numbers with the system's private key to produce an activation code, but only after the user authenticates to the card using a PIN[3] (Personal Identification Number). The card would be programmed to only produce 2 or 3 activation codes before erasing the key from its memory thus rendering the card useless. This is a desirable feature when trying to prevent abuse, in the unlikely event that an attacker steals the card and the card's unique PIN, the number of activation codes that can be generated is contained. As an added measure, the card will erase the key if it is sent too many invalid PINs[4] or the card fails a number of self-tests[5].

Finally, someone that is broadcasting un-authorized activation codes on the Digital Receive Frequency (DRF) can ultimately be tri-angulated and located using the same techniques used in a DF search operation.

[3] Similar to a PIN used at a bank machine. One must have the card and know the PIN in order to produce an activation code.

[4] Prevent the guessing of a card's unique PIN.

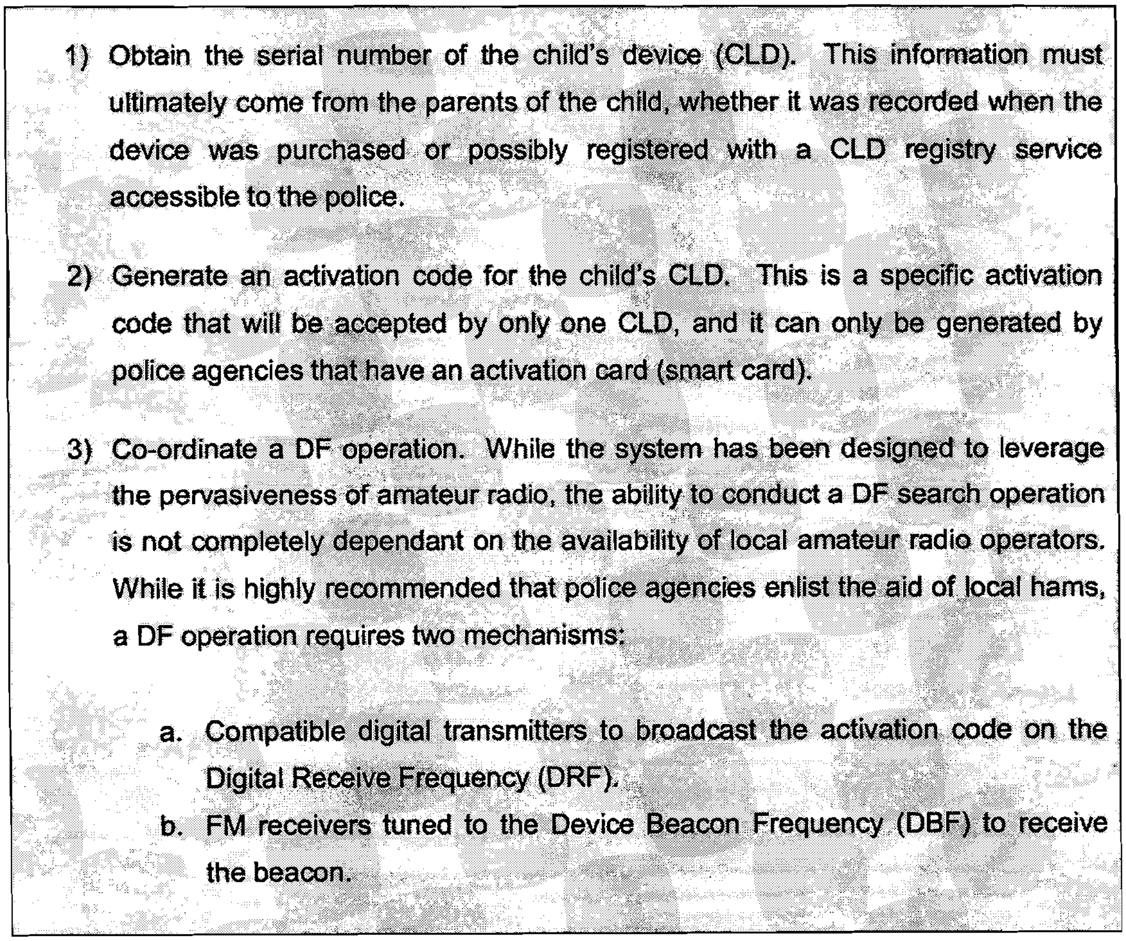
[5] Attempt to prevent "side channel" attacks.

All of these controls are required elements of the system; they protect the system against abuse using a layered security approach that is designed safeguard a child from unauthorized DF attempts using the child's device (CLD).

5 Description of Police Response

Initiating a search for a missing child is done at the sole discretion of the local police department. This system, the device (CLD) and ham radio operators are all intended to be facilities that aid police in quickly recover the missing child. Police will co-ordinate and ultimately control a DF operation, with amateur radio volunteers playing a critical and supportive role.

In order to initiate a DF enabled search for a missing child, the police will be required to:



1) Obtain the serial number of the child's device (CLD). This information must ultimately come from the parents of the child, whether it was recorded when the device was purchased or possibly registered with a CLD registry service accessible to the police.

2) Generate an activation code for the child's CLD. This is a specific activation code that will be accepted by only one CLD, and it can only be generated by police agencies that have an activation card (smart card).

3) Co-ordinate a DF operation. While the system has been designed to leverage the pervasiveness of amateur radio, the ability to conduct a DF search operation is not completely dependant on the availability of local amateur radio operators. While it is highly recommended that police agencies enlist the aid of local hams, a DF operation requires two mechanisms:

   a. Compatible digital transmitters to broadcast the activation code on the Digital Receive Frequency (DRF).
   b. FM receivers tuned to the Device Beacon Frequency (DBF) to receive the beacon.

Figure 5-1 : Police Response

At a minimum, 3.a and 3.b above are required for a naïve DF operation and do not require the participation of the amateur community. However, by utilizing more sophisticated logistics combined with the communications expertise of an organized local amateur radio organization the likelihood of a successful DF operation has greater potential.

6 Description of Ham Response

Police decide on the degree and level of involvement of ham volunteers involved in a search. The main goal of Police is to quickly recover a missing child and if the local amateur group has a reputation for professionalism, Police may be more willing to depend on ham services during the time critical search operation. Regardless of DF training and level of preparedness, some of the activities amateurs may be asked to lend their expertise include:

1) Initiating their local Ham emergency call-up tree, to provide the police with an immediate source of volunteers and readily accessible communications expertise.
2) Wide area activation code broadcasting through the use of club repeaters.
3) Mobile localized broadcasting of an activation code.
4) Mobile localized search and receive of the device (CLD) over the Device Beacon Frequency (DBF), using both DF and non-DF receivers.
5) Participation in an APRS enabled, controlled DF search operation.
6) Participation in a communications hub or command center that must handle the logistics of a DF enabled search.

Figure 6-1 : Ham Response Activities

A more detailed framework for ham participation in a search is included in Appendix A. The above figure is a high level summary of that framework.

7 'Activation Code' Details

The activation code is a combination of the device's (CLD's) unique serial number, the activation card's[6] serial number and a digital signature. By including these data elements in the activation code it can be ensured that:

1) Only one device (CLD) is authorized over-the-air to start transmitting even though all CLDs within range will receive the code.
2) The police agency responsible for generating the activation code can be traced using the activation card's unique serial number.[7]
3) The activation code was generated by an authorized police agency.

The digital signature portion of the activation code ensures that the code is authentic (from a valid source) and was not corrupted during transmission. It is calculated using a form of mathematics called public key encryption[8] that is described in the following procedure:

1) The device serial number and smart card serial number are concatenated to produce the message M. (M = <CLD SN>|<SmartCard SN>)
2) M is hashed using SHA-1 to produce 20-bytes of digest D. (D = Sha-1(M)).
3) Choose one of the following digital signature mechanisms:
   a. D is signed using a 4092-bit RSA private-key producing 512 bytes of signature S. (S = RSA-PKCS1(D, PrivateKey))
   b. D is signed using a 239-bit ECDSA private-key producing 60 bytes of signature S. (S = ECDSA(D, PrivateKey, 239-bit Curve))
4) The activation code (AC) is created by concatenating M and S. (AC = M | S)

Figure 7-1 : Constructing an Activation Code

[6] The smart card used by police to produce activation codes.

[7] Since the activation card's serial number is an integral component of the activation code, a CLD will not accept a code with a "fake" activation card serial number component.

[8] Typically, the use of cryptography within amateur radio is forbidden since all communication must be public. In this case the cryptographic mechanisms are being used for data integrity not secrecy. An activation code can be read (and verified) by anyone who receives it.

Upon receiving the activation code, the device must process the code using the following procedure:

1) Parse the activation code into sub-components M (Message), S (Signature), CLD-SN (Device Serial Number) and SC-SN (Smart Card Serial Number).
2) The device (CLD) must compare its own serial number to that in the activation code CLD-SN. If the serial numbers do not match than the CLD will ignore the activation code and not process it any further.
3) M is hashed using SHA-1 to produce 20 bytes of digest D. (D = Sha-1(M)).
4) D and S are passed to the signature verification function along with the Public Key of the signer to determine if signature is valid. (Boolean-Valid = Verify(D, S, PublicKey).
5) If the signature is valid, the activation code is accepted thereby authorizing the device to enter a transmitting state.

Figure 7-2 : Processing an Activation Code.

Addendum A: Framework for a controlled DF search operation.

Roles And Classifications:

ACC	"Abduction Communications Center" is an individual or a collective group of amateurs that provide logistical support to a DF search operation. From the perspective of all ham volunteers participating in the search, the ACC is the net controller, the communications hub and the operational leader. Search groups register with the ACC who is then responsible for directing their movements. The ACC should be constantly updated with each search group's geographical location.
Class 1 Search Group	A class 1 search group has equipment to simultaneously listen to the device beacon frequency (DBF) and communicate with the ACC. This is the base requirement for actively participating in a DF operation.
Class 2 Search Group	A class 1 search group with digital transmit, and APRS capability.
Class 3 Search Group	Class 2 with D, M and > 30 Watt designators. This class implies a consistent quality of service. A search group that identifies as class 3 is expected to be able to remain class 3 for the duration of the search. For example, if the group leaves their vehicle, they are expected to maintain D and >30 Watts designators (as well as digital capabilities) regardless of having to operate on battery power.

Optional Class Designators

B	Operating on battery power, limited transmit capability.
D	Outfitted with a directional antenna, capable of producing a vector.
M	The search group is mobile. The group is equipped with a vehicle, or the vehicle is near by allowing for group relocation. The group can operate on foot and is not tied to the vehicle.
V	The search group's equipment is tied to a vehicle. Note that this designator is mutually exclusive with the M designator.

X	Search group has a police escort.
<N> Watts	The final class designator must be the search group's sustainable power output while transmitting a digital signal on the DRF. Implicitly, class 1 search groups can drop this class designator.
Example:	*VA3BPN is Class2 Delta Mike X-Ray 30 Watts*

Phases of a DF Search Operation

Phase 1: Mobilization

1) Once police have determined that a DF enabled search for abducted child is warranted and that help from the amateur community would be advantageous, the police should request assistance from the nearest local amateur radio club as soon as possible. Amateur clubs will typically have an emergency call up tree that will allow them to quickly respond to a request for volunteers. The efficiency and timeliness of the amateur response will indicate to police what level of professionalism and experience the local amateurs are capable of providing during a DF operation. This initial stage is critical to the DF operation as police need to quickly gather communications expertise as well as search volunteers and amateurs need time to mobilize within a period of time that is critical to a successful search.
2) Police should consider issuing an 'Amber Alert' if the service is available locally. Using the Amber Alert, police would distribute the Device Beacon Frequency (DBF) to the public so that citizens using police scanners and other types of receivers can monitor the DBF and contact a special police call center if a modulated signal is detected. Conversely, police should also consider that an Amber Alert may tip off the abductor that the child is carrying a device (CLD).
3) A communications hub must be established; preferably the hub will be located within the police command centre so that communication between the police and the ACC can be efficiently facilitated.
4) The ACC must identify, establish and position search teams within a geographic area that police want to concentrate the efforts of search volunteers. The ACC must consider many factors for initial placement of DF teams, with wide transmit coverage of the activation code being the primary concern at the beginning of the

DF search. Class 3 search teams and repeaters would be the preferable broadcast agents.

Phase 2: Wide Search

5) The activation code should ideally be broadcast using a combination of repeaters and class 3 search teams to effectively reach the device and limit collisions on the Digital Receive Frequency (DRF). Detecting the beacon on the Device Beacon Frequency (DBF) is open to any receiver operator including search teams, police and civilians.
6) The ACC should be aware of transmit and receive ranges of search teams so that by using APRS tracking software the ACC can 'paint' a search area specified by police, ensuring a search area receives appropriate coverage.

Phase 3: Triangulation And Containment

7) Once a tone has been detected on the Device Beacon Frequency (DBF), transmission of the activation code on the Digital Receive Frequency (DRF) can cease and the ACC can concentrate the efforts of search teams on triangulating the device in order to determine a position.
8) There is a strong likelihood that the device will be moving. This implies that the device's signal will be positioned at different locations over a period of time, or the device's signal may disappear if it moves underground or deep into a building. The ACC must be acutely aware of the search's surrounding landscape, geographical and urban properties.
9) The ACC should give the more experienced fox hunters a large degree of freedom to track down the beacon, while positioning less experienced lower classified search teams in a containment parameter on the chance that the signal escapes the more active DF teams.

Phase 4: Device Encounter

10) Once the beacon tone is discovered on the Device Beacon Frequency (DBF), DF search teams will likely hone in and position the device quickly. It is absolutely imperative that DF search teams do not encounter the device or engage an abductor. This is strictly in the domain of the police, who have the training and resources to handle such a situation.

11)The ACC should ensure that all search teams within a 5 km radius of the suspected device position have a police escort. At this point in the DF operation the ACC should be in constant communication with police operational directors.

Acronyms

ACC	Abduction Communication Centre
APRS	Automatic Position Reporting System
CLD	Child Locator Device
DBF	Device Beacon Frequency
DRF	Digital Receive Frequency
DSS	Digital Spread Spectrum
ECDSA	Elliptic Curve Digital Signature Algorithm.
PIN	Personal Identification Number
PKCS1	Public Key Cryptography Standard #1. Owned by RSA.
RSA	A public key cryptographic scheme, named after the authors Ronald Rivest, Adi Shamir, and Leonard Adleman.
TNC	Terminal Node Controller

References

Douglas R. Stinson *Cryptography Theory and Practice, Second Edition,* Chapman & Hall/CRC, 2002

Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone *Handbook of Applied Cryptograph*, CRC Press, 1997

RSA Laboratories *PKCS #1 v2.1: RSA Cryptography Standard,* RSA Laboratories, June 14, 2002, ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf

Technical Information regarding Schlumberger's programmable "JavaCard" smart card can be found at http://www.cyberflex.com/Support/Documentation/documentation.html