3GPP2 SC.R5001-0

Version 1.0

Version Date: 10 June 2004

3RD GENERATION PARTNERSHIP PROJECT 2 "3GPP2"

3GPP2 Vision

Revision History

Revision	**Description**	**Date**
Version 1.0	Initial publication version	10 June 2004

TABLE OF CONTENTS

1 INTRODUCTION, DOCUMENT SCOPE, AND LONG-TERM VISION

The Vision of 3GPP2 is to continue cdma2000®[1]'s evolution in delivering value-added applications and services to the user. Enhanced capabilities such as wireless seamless mobility, portability, and location information are some of the enablers for the future of wireless technology. The evolution should put emphasis on backward compatibility for the cdma2000 Radio interface as well as providing compatibility and interoperability with existing and emerging wireless/mobile technologies. The ultimate goal is to provide an architecture that allows for common services and a universal set of applications to the user.

This document looks at long-term vision that is beyond what is described in the 3GPP2 Evolution document [1]. The document attempts to provide guidance to 3GPP2 on new capabilities, features, and interoperability requirements. It will also provide an evolution path for the core network and RAN elements including new interfaces and technologies that could be considered or incorporated into the 3GPP2 Evolution plan.

The long-term vision of 3GPP2 is a work in progress. The details of this vision will gradually emerge from extensive, worldwide cooperative research in several key areas outlined in the subsequent sections of the document. The fundamental premise of this vision is that the market needs will drive the long-term evolution of wireless networks. Many new concepts and technologies are likely to emerge out of research and be subjected to the scrutiny of both the wireless industry and the market. 3GPP2 will take the sensible approach of adopting a vision based on future-proof concepts and technologies that are likely to succeed in the market place. The following sections of this vision document provide insight into the more prominent concepts and trends that are of interest to 3GPP2.

2 ACRONYMS, ABBREVIATIONS, AND TERMINOLOGY

3GPP	Third Generation Partnership Project	www.3gpp.org
3GPP2	Third Generation Partnership Project 2	www.3gpp2.org
AAA	Authentication, Authorization, and Accounting	
ARPU	Average Revenue per User	
AMI-C	Automotive Multimedia Interface – Collaboration	www.ami-c.org
BCMCS	Broadcast Multi-Cast Services	
DVB	Digital Video Broadcast	
ERTICO	ERTICO is a Europe-wide, not-for-profit, public/private partnership for the implementation of Intelligent Transport Systems and Services (ITS).	www.ertico.com

[1] cdma2000® is the trademark for the technical nomenclature for certain specifications and standards of the Organizational Partners (OPs) of 3GPP2. Geographically (and as of the date of publication), cdma2000® is a registered trademark of the Telecommunications Industry Association (TIA-USA) in the United States.

IETF	Internet Engineering Task Force	www.ietf.org
IP	Internet Protocol	
ITU	International Telecommunications Union	www.itu.int
ITU-T SSG	ITU Telecommunications Standardization Sector Special Study Group	www.itu.int/ITU-T
MAC	Media Access Control	
MMD	Multi-Media Domain	
OASIS	Organization for the Advancement of Structured Information Standards	www.oasis-open.org
OMA	Open Mobile Alliance	www.openmobilealliance.org
OSA	Open Service Access	
Parlay	The Parlay Group	www.parlay.org
QoS	Quality of Service	
RAN	Radio Access Network	
RF	Radio Frequency	
SOAP	Simple Object Access Protocol	
SDR	Software Defined Radio	
TMN	Telecommunication Management Network	
VoIP	Voice Over IP	
W3C	World Wide Web Consortium	www.w3c.org
WLAN	Wireless Local Area Network	

3 REFERENCES

[1] 3GPP2 S.R0038-0 The 3GPP2 Evolution Document

[2] 3GPP TR 21.902 Evolution of 3GPP System

[3] Recommendations from the April 3-4, 2002 IP CN Harmonization Workshop (S00-20020415-004B)

4 RESEARCH IN APPLICATIONS

Applications are one of the main drivers for enhancements to wireless systems. The goal of the 3GPP2 activity is to provide a common set of services, which support diverse applications for the users, independent of which access network they are using. 3GPP2 will work with organizations such as 3GPP, OMA, IETF, ITU-T NGN, and others that may be applicable to develop this common set of services. 3GPP2 will determine what aspects it will standardize. When appropriate, 3GPP2 will establish liaison relationships with external organizations to develop applications. This harmonized set of applications and services will then be used by 3GPP2 to develop the specifications and technologies to support them.

4.1 User Applications

Research in user applications that demand asymmetric transmission resources could benefit operators by allowing overall network throughput in the forward and reverse links to be commensurate with inherent radio resources capabilities. Examples of asymmetric applications include BCMCS and web-browsing applications. Both are more demanding on the forward link throughput.

4.2 Device Capabilities

For further study

4.3 DVB Application

For further study

4.4 Network Services

Network functions, which may include call/session control, routing, charging/billing functions, authentication and authorization services, roaming, and access to data and messaging bearers such as packet data, SMS and MMS, are collectively referred to as network services. Increasingly, operators will rely on the massive base of 3rd-party application providers such as ASPs (Application Services Providers), service aggregators, resellers, and IT application developers, for the rollout of value added services that make use of network services.

To control the access to these valuable network assets by 3rd-party application providers in a secure and reliable manner, standards-based service architectures such as Parlay/OSA have been developed. Initially designed for 3rd-party control of voice services, Parlay/OSA has evolved to support data services functionality and has defined interfaces, or APIs, for application access to a variety of network functions (referred to as Service Capability Features, or SCFs). A key enabler for more pervasive implementation of network services will be Web services technologies, based on SOAP/XML/HTTP. Network services can be represented as Web services for their publication, discovery and invocation. Standards-based solutions for interoperable, reliable and secure Web services are emerging but are not yet mature. In addition, as shown in OMA, there is strong interest by operators in the concept of execution policy and workflow, to support flexible service control during network service invocation. 3GPP2 should work in concert with OMA and pertinent IT-centric SDOs (e.g. W3C and OASIS) in developing the evolution of network services enabling technologies and architectures.

4.5 Location Services

3GPP2 will build upon its background and success in location services to extend the ability to determine the location of a mobile station to new advanced location services such as:

- Network optimization,
- Predictive traffic loading,

- Commercial services, etc.

Location service is a key unique wireless service. Strong multi-way interaction will be established with applicable organizations such as IETF and OMA.

The utility of location-based services is expected to be considerably enhanced when they are offered over IP interface, and when fast cdma2000 transmission speed can be taken advantage of. This will allow enhancement on applications being accessible from devices connected to the Internet. Enterprise applications are of particular interest. The combination of these elements will also allow fast map download and update. The economy and accessibility of location-based services will be enhanced by advanced techniques that manage assistance delivery and control location reporting for optimized network and application performance.

5 RESEARCH IN SERVICE ENABLERS

Service Enablers should be able to support the provision of applications and services across multiple access networks.

5.1 Security

Security is an essential capability that is used to support the deployment of applications and services. Security must be addressed, not only for the cdma2000 radio interface, but also for end-to-end service provisioning.

Security capabilities must be flexible in order to provide various levels of security appropriate to the service/application being provided. With the deployment of IP services and applications, security becomes much more important to the user, the operator and the service provider.

5.1.1 Security in IP Based Network

Since signaling transport may not be physically separated from user data transport, security issues related to IP are much more critical and difficult than those in existing networks. Since all IP packets from various users are transmitted over common links, it is expected that IP-based applications and services will support application security independent of network security. Users have an expectation of privacy and systems must provide that privacy. Operators must protect the network and provide transparency for user specific protection mechanisms.

Internet applications such as e-mail, web browsing, and multimedia streaming have already been implemented in mobile stations, and additional ones are expected to come to the mobile environment. Therefore, threats to the Internet infrastructure and to Internet applications would also become threats to future mobile environments, and similar security mechanisms as applied to the wired Internet will be necessary to protect mobile environments.

5.1.2 Scalable Security Architecture Across All Devices/Spaces

Security provides the foundation for two of the most important customer concerns, trust and privacy. Participants in the value chain where products are deployed, from content and service providers to end customers/consumers, have a very high expectation that the devices and systems developed will perform their intended functions, and only their intended functions. Users authorized to access those functions (trust), personal information, personal and network communications, and any other data or content will be protected from undesired or unapproved use by others (privacy).

The need to ensure trust and privacy is independent of whether a device or system is connected to a wired network, a WLAN, wide-area cellular network, or any sort of hybrid network, or is simply a stand-alone device. Likewise, the assurance of trust and privacy is independent of which generation of networks or devices it is implemented for. However, the requirements and capabilities necessary for providing the appropriate level of security have become more complex as networking technology has advanced, requiring security support for complex personal and financial transactions, and support for the secure, private delivery of value-added content and services. Of course, these issues are not new, and they are being addressed across a broad spectrum of industry- and technology-specific standards bodies.

5.1.3 Access Security

Security procedure shall be performed efficiently to minimize negative impact on user applications and maximize user service satisfaction.

Future user authentication may include local authentication between a user and a terminal based on biometrics e.g., a specific feature of an individual such as voice, fingerprint or iris validation. These capabilities may complement the traditional user authentication methods.

5.1.4 Seamless roaming across heterogeneous networks

Roaming between networks, or more specifically, seamless roaming between different access technologies, adds yet another level of complexity to the security equation, and one which has only been addressed in the industry to a limited degree. Seamless roaming between heterogeneous networks (e.g. wide-area cellular to WLAN, or wireless to wired) has typically been possible only if the networks are all owned/controlled by the same entity, e.g., they encompass a single administrative domain. In a future world of heterogeneous networks, where seamless roaming between different types of access networks and across administrative domains is possible, the trust and privacy equation becomes even more complex. This complexity requires developing a scalable security/trust architecture consisting of security building blocks that can be implemented at the silicon, device or system level. Because this architecture would enable a common security framework which could stretch across devices in all spaces, it would enable a high level of security interoperability, and therefore the assurance of trust and privacy, as devices roam across networks and administrative domains, thereby enabling secure seamless roaming in a true heterogeneous network.

5.1.5 Application level of security

5.1.5.1 Support for certificate based security

Future applications such as m-commerce and m-transactions will require certificate-based security. The mobile station must be able to support subscriber-based and server-based certificates.

5.1.5.2 Contents right protection

It is expected that various multimedia contents will be widely available to mobiles where the content copyright(s) must be securely protected. Methods of protecting the copyrights of digital contents are expected to be developed (e.g., Digital Rights Management).

5.1.5.3 End-to-end security

End-to-end application layer security (authentication, privacy and integrity) may be required independently of the underlining network architecture. Therefore it is expected that the network architecture and the underlining transport mechanisms will be transparent to the application layer security deployed to support end-to-end security.

5.1.6 Security for short range interfaces

Several short-range interface technologies e.g., IrDA and Bluetooth are already available. In the near future, many applications may use those interfaces to provide connectivity between a mobile station and various external devices such as display screen, external speakers, pen interface, sensors, etc. Therefore, security over those interfaces should be designed to ensure similar security levels as those available for cellular technology.

5.1.7 Robustness against potential attacks

Network spamming has caused a lot of problems with Internet traffic today. The IP industry has been spending a lot of efforts trying to improve this situation but has had limited success. Due to radio bandwidth limitations and airtime cost, this problem is magnified for a wireless network operator and subscriber.

Denial of Services (DoS) attacks or Distributed Denial of Services (DDoS) attacks and packet spoofing are becoming common on the Internet as well as to mobile systems.

The next generation 3GPP2 All-IP core network should provide an effective solution to minimize those damages and limit the impact to its end users. 3GPP2 will work with other industrial fora to develop the best solutions to protect the network operator and end users from potential attacks.

5.2 Network Management/Service Management

Network Management refers to the full range of activities that the network operator must perform to ensure the reliable, secure delivery of network services to its customers. In the ITU TMN standard terminology, it covers the Fault, Configuration, Accounting, Performance and Security (FCAPS) functionalities in the management of a telecommunications network. Network management is also concerned with the addition, configuration, optimization, upgrade and repair of network elements. Service management has to do with the provision of services to end customers at a promised level of performance (Service Level Agreements) as well as ensuring the security and privacy of personal information that is being carried over its networks. All of these must be done in a way that ensures that the carrier can generate revenue and profits for the services it provides (*including that the carrier may charge for these network and service management services*). The goal of every network owner is to reduce operational cost and maximize revenue. This means that the focus is on the speed of introduction for new and innovative services that in turn drive ARPU. Another goal is to reduce workforce and overall operational complexities. This means ease-of-use of administrative functions and plug-and-play network components that can be developed. In these times when QoS is a major concern and differentiator, the ability to administer Service Level Agreements is also a critical requirement.

Following scenarios are listed which adding additional challenges to network management, service provisioning, authentication and accounting.

- With the advent of advanced telecommunications systems and the promise of rich, complex, multimedia services, the functionalities for network and service management become a lot more complex. In addition to addressing the performance, reliability and scalability of very large networks, the ability to authenticate the user as he/she roams across future communications networks and legacy networks and to account, aggregate and bill for content-based, multimedia services become key new priorities for the operator.

- Disparate access networks will converge to provide the best services to the end user whether they are at home, at work, or in transit. The idea is to exploit the best services offered by each radio network to create innovative services that offer compelling life-style changes to the consumer. This in turn enhances the revenue of the operator and the service provider. Cellular and WLAN convergence is one possible example of this scenario. The convergence of cellular and broadcast networks also presents compelling possibilities without violating the current regulatory framework.
- Such convergence will likely cause new business models to emerge. One example is that of many operators and service providers freely share physical radio networks as well as content and applications across the personal, car, home and enterprise spaces. Convergence will also necessitate the creation of new user devices.
- Another potential future communications scenario is that of intelligent sensors and devices everywhere at home, in commercial settings as well as in public places.

To address these challenges key topics for Network Management are:

- Management of multi radio technology networks
- Always on, always available systems and applications
- Seamlessness in the user experience
- Exponential growth in the number of network nodes
- New business models to be accommodated

An additional challenge is that these complexities need to be accomplished at the lowest cost and within a rapid service deployment environment.

Some answers to these challenges can be found by addressing solutions for:

- End-to-end service and network management, including QoS
- RF self-configuration (e.g. within the RF domain)
- Plug-and-play installation
- Auto-configuration
- Self-healing
- Auto service provisioning
- Ad-hoc networking
- Seamless AAA (Authentication, Authorization and Accounting) for roaming
- RF resource management
- Content management (i.e. content as a network resource)
- Billing aggregation

- Micro-billing (e.g. charging for per usage services)

5.3 Quality of Service (QoS)

End-to-End QoS is an essential capability that supports the deployment of a set of applications and services that require better than best-effort service end-to-end. In a cdma2000 system, End-to-End QoS must be addressed not only for the cdma2000 system but also for End-to-End service provisioning. It must be flexible to provide the various levels of QoS that may be requested by applications and services.

The envisioned cdma2000 QoS capability should enable the system to vary QoS treatment depending on user, application, and service needs, and allow the system to compute metrics that measure how closely the delivered QoS level meets the requested QoS level.. The ability to control QoS based on these metrics will allow operators to offer service tiers backed by measurable service parameters. Besides increasing high-value service revenues and customer satisfaction, differentiated QoS will enable operators to better control and more efficiently plan capital expenditures for network growth. It is envisaged that the QoS needs of an operator's "premium" customers will be a prominent factor in future network capacity planning.

5.3.1 User Tiers

The cdma2000 system should be designed to recognize user traffic with higher priority and reorder packets based upon the packet's priority.. User tiers may be based on preferential QoS treatment. The system should be able to check a subscriber's QoS profile on a per session basis and match it to an appropriate QoS tier of service and the needs of the specific application.

5.3.2 Application QoS Continuum

Another aspect of QoS is the ability to treat applications differently, for example, based on delay requirements. Delay sensitive traffic (VoIP, videoconferencing, low-latency games, instant messaging, etc.) will receive higher priority treatment than more delay-tolerant traffic (web-browsing, e-mail, etc.). Preferential QoS treatment is applicable to both a single user and to multiple users. An extremely large set of QoS attribute values/value ranges (on availability, delay, jitter, packet loss, throughput, etc.) will be necessary to characterize the wide range of applications expected to run in a cdma2000 system. These values may depend not only on the application, but also other factors such as the user's service tier, or network conditions. Fine-grained characterization will enable QoS differentiation of applications frequently considered to belong to a single category. Although both voice telephony and videoconferencing applications have stringent low delay requirements, they have different bandwidth needs. Interactive games may vary in delay requirements.

6 RESEARCH IN TECHNOLOGY ENABLERS

There are a number of advanced technologies that can potentially enhance the lower layer performance that are currently being studied. The following is an initial list of these technologies.

6.1 Antennas

Advanced antenna technology can provide benefits in the evolution of cdma2000. The technology developed by 3GPP2 should be flexible enough to allow for a range of products, each with differing limits on the number and type of antennas supported as well as transceiver complexity. Environmental, aesthetic, ergonomic, regulatory, and manufacturability factors should also be considered when specifying advanced antenna specifications.

6.2 Software Defined Radio (SDR)

Software Definable Radio (SDR) can be an important technology for future communications systems. Flexibility is the key attribute of an SDR. For example, a radio could be upgraded with new software, have the capability of reconfiguring to operate on different technologies, or have a much less complicated hardware design accommodating multiple access technologies (e.g., multi-mode devices).

Research on SDR technology could lead to the following capabilities:

1. To upgrade radio software remotely and wirelessly. This might include software version upgrades from the application level as well as the air interface protocol stack.
2. A radio to reconfigure itself dynamically based upon the access technology needed at the time.
3. To realize common terminal platforms across multiple access technologies or performance/capability tiers.
4. To develop common wireless access device platforms (e.g., base stations).

7 RESEARCH IN THE IP CORE NETWORK

3GPP2 will work with other organizations to develop a common IP Architecture for wireless systems that is independent of radio access technologies.

The evolution of 3GPP2 is towards all-IP networks and IP-based services. The industry needs robust and well performing packet data networks as these serve as the foundation for all-IP and IP-based services. In development of advanced IP networks, 3GPP2 will:

- Describe an MMD core network as an IP-based network with flexibility to enable implementation and deployment as part of a managed-IP network or as an extension of the Internet, thereby allowing a range of options to operators, reflecting MMD network open architecture, and offering enhanced packet data and multi-media session capabilities,
- Use proven Internet protocols and popular Internet services unaltered whenever possible or enhanced when applicable.
- Take into account the evolving business models for advanced packet data services.
- Take into account radio channel physical characteristics in the development of all-IP networks.
- Take into account the 3GPP Evolution Plan [2] in regard to a harmonized IP core network between 3GPP and 3GPP2.

- Take into account the development and publications from the ITU-T SSG and other related ITU-T SG studies (e.g. www.itu.int/ITU-T/).

7.1 Wireless IP Networking Architectures

One of the key objectives of migration to IP based core network solutions, is to take advantage of packet data communication techniques that have proven themselves in various forms of access, and apply them as broadly and as deeply as possible in offering cdma2000 networking solutions. This will allow system integrators and operators to use off-the-shelf equipment to configure wireless networks. Inherent in the IP solutions is the distributed functionality of network elements. Broad adoption of that functionality will result in increased network reliability without planned redundancy of overly centralized solutions. This approach will offer autonomously configurable, if not self-configurable network solutions.

The approach is consistent with the goal of scalability, which allows operators to plan network growth better, without committing excessive up-front capital. This in turn will offer operators ability to be more flexible in responding to fast changes in the technology, demand, and competitive environment.

In the purely technical sense, the omnipresent IP networking approach will demand:

- Research in new techniques for discovery of network/service resources,
- Research in distributed resource techniques and optimum distribution of network/service resources
- Research in distributed mobility management techniques
- Operational research allowing planning to meet complex and non-uniform performance goals

8 RESEARCH IN THE PHYSICAL AND MAC LAYERS

The industry requires robust and well performing air interfaces as the foundation for wireless services. 3GPP2 will develop specifications to ensure efficient use of limited resources such as spectrum bandwidth and mobile transmitter power.

Backward compatibility with cdma2000 and its variants is a key criterion for the evolution of cdma2000 radio interfaces as they evolve.

3GPP2 will work towards further harmonization in the development of radio interfaces.

The following areas are important for evolution:

- Development for micro-cells
- Development/enhancement to support repeaters
- Development to support mobile stations using multiple and/or advanced antenna
- Development for packet data services
- Development for higher voice capacity

In the development of advanced air interfaces, 3GPP2 should take into account the development and publications from the ITU-R WP8F Vision Group and other such studies.

9 RESEARCH IN CODECS

Multimedia applications are an important part of the future for cdma2000. The development and support of interoperable audio, video, and wideband codecs should be a part of the 3GPP2 vision.

- The deployment of advanced video coding which significantly enhances video quality and capacity, provides wireless-friendly error resilience, and harmonizes video related applications across future wireless technologies is critical.
- A harmonized set of applications and services will benefit from the development and standardization of a high quality bandwidth-efficient audio codec that is designed to meet the demands of a wireless environment. The ability to operate at multiple bit rates might be considered. Similarly, a codec that performs well with non-speech input might be desirable. One example application for this codec is audio streaming.
- There will be continued evolution of wideband codecs that provide high-fidelity voice services. System issues such as the need for tandem free operation, VoIP, etc. are required should be supported.

10 RESEARCH IN USER INTERFACES AND THE USER EXPERIENCE AS THEY RELATE TO STANDARDIZATION ACTIVITIES

3GPP2 will, when appropriate, create liaisons with organization developing information management standards (e.g. AMI-C, ERTICO, etc.)