**Overview**

A VPN\(^1\) authentication system for next-generation networks (NGNs), called “AAA\(^2\),” —for providing RADIUS\(^3\) user authentication (i.e., terminal authentication) in response to multiple VPNs on an NGN— was developed. By providing (1) high-level conformity needed for NGN-VPN services, i.e., interoperability (assumed to be with various corresponding legacy-network termination equipment) and handling of line-identification information of legacy networks/NGNs, (2) high extensibility for flexibly handling future service expansion and (3) service continuity during hardware faults and occurrence of disasters, redundancy of equipment and facilities between distant regions can be created at low cost.

**Features**

- Highly secure VPN authentication based on line-identification information of NGNs and legacy networks is achieved
- Method for synchronization of data between remote regions by using low-cost database middleware
- RADIUS authentication architecture that can flexibly handle additional functions
- VPN session information can be provided for host Applications
- Systems can still be provided when architecture is degenerative

**Application scenarios**

- Application as VPN-service authentication system possessing high security and high availability
- VPN session information is utilized for authentication and accounting regarding application services provided on VPNs
- Provision of multi-factor authentication systems flexibly combining arbitrary attributes
- User-authentication capability for newly initiated small-scale services is made possible at low cost

---

\(^1\) VPN: Virtual Private Network  
\(^2\) AAA: Authentication, Authorization, Accounting system  
\(^3\) RADIUS: Remote Authentication Dial In User Service