ETSI GR IP6 031 V1.1.1 (2020-11)

IPv6 Security, Cybersecurity, Blockchain

Disclaimer

The present document has been produced and approved by the IPv6 Integration (IP6) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGR/IP6-0031

Keywords
blockchain, cybersecurity, internet, IPv6, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) IPv6 Integration (IP6).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document gives the outline of deployment of IPv6 security, Cybersecurity, Blockchain an DatablockMatrix.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] "Are you sharing the same IP address as a criminal? Law enforcement call for the end of carrier grade NAT (CGN) to increase accountability online", October 2017.

NOTE: Available at https://www.europol.europa.eu/newsroom/news/are-you-sharing-same-ip-address-criminal-law-enforcement-call-for-end-of-carrier-grade-nat-cgn-to-increase-accountability-online.

[i.2] IETF draft-chakrabarti-nordmark-6man-efficient-nd: "IPv6 Neighbor Discovery Optimizations for Wired and Wireless Networks", February 2015.

[i.3] IETF draft-ietf-dhc-sedhcpv6: "Secure DHCPv6", February 2017.

[i.4] IETF draft-ietf-opsec-ipv6-eh-filtering: "Recommendations on the Filtering of IPv6 Packets Containing IPv6 Extension Headers", July 2018.

[i.5] IETF draft-ietf-v6ops-ula-usage-considerations: "Considerations For Using Unique Local Addresses", March 2017.

[i.6] IETF draft-kampanakis-6man-ipv6-eh-parsing: "Implementation Guidelines for parsing IPv6 Extension Headers", August 2014.

[i.7] IETF draft-thubert-savi-ra-throttler: "Throttling RAs on constrained interfaces", June 2012.

[i.8] IETF RFC 1918 (February 1996): "Address Allocation for Private Internets".

[i.9] IETF RFC 2131 (March 1997): "Dynamic Host Configuration Protocol".

[i.10] IETF RFC 2460 (December 1998): "Internet Protocol, Version 6 (IPv6)Specification".

NOTE: Obsoleted by IETF RFC 8200.

[i.11] IETF RFC 2529 (March 1999): "Transmission of IPv6 over IPv4 Domains without Explicit Tunnels".

[i.12] IETF RFC 2740 (December 1999): "OSPF for IPv6".

[i.13] IETF RFC 2784 (March 2000): "Generic Routing Encapsulation (GRE)".

[i.14] IETF RFC 2827 (May 2000): "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing".

[i.15] IETF RFC 2866 (June 2000): "RADIUS Accounting".

[i.16] IETF RFC 3756 (May 2004): "IPv6 Neighbor Discovery (ND) Trust Models and Threats".

[i.17] IETF RFC 3924 (October 2004): "Cisco Architecture for Lawful Intercept in IP Networks".

[i.18] IETF RFC 3971 (March 2005): "SEcure Neighbor Discovery (SEND)".

[i.19] IETF RFC 3972 (March 2005): "Cryptographically Generated Addresses (CGA)".

[i.20] IETF RFC 4193 (October 2005): "Unique Local IPv6 Unicast Addresses".

[i.21] IETF RFC 4293 (April 2006): "Management Information Base for the Internet Protocol (IP)".

[i.22] IETF RFC 4301 (December 2005): "Security Architecture for the Internet Protocol".

[i.23] IETF RFC 4302 (December 2005): "IP Authentication Header".

[i.24] IETF RFC 4303 (December 2005): "IP Encapsulating Security Payload (ESP)".

[i.25] IETF RFC 4364 (February 2006): "BGP/MPLS IP Virtual Private Networks (VPNs)".

[i.26] IETF RFC 4381 (February 2006): "Analysis of the Security of BGP/MPLS IP Virtual Private Networks (VPNs)".

[i.27] IETF RFC 4443 (March 2006): "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification".

[i.28] IETF RFC 4649 (August 2006): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option".

[i.29] IETF RFC 4659 (September 2006): "BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN".

[i.30] IETF RFC 4798 (February 2007): "Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)".

[i.31] IETF RFC 4861 (September 2007): "Neighbor Discovery for IP version 6 (IPv6)".

[i.32] IETF RFC 4864 (May 2007): "Local Network Protection for IPv6".

[i.33] IETF RFC 4890 (May 2007): "Recommendations for Filtering ICMPv6 Messages in Firewalls".

[i.34] IETF RFC 4941 (September 2007): "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".

[i.35] IETF RFC 5340 (July 2008): "OSPF for IPv6".

[i.36] IETF RFC 5635 (August 2009): "Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)".

[i.37] IETF RFC 5952 (August 2010): "A Recommendation for IPv6 Address Text Representation".

[i.38] IETF RFC 6092 (January 2011): "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service".

[i.39] IETF RFC 6104 (February 2011): "Rogue IPv6 Router Advertisement Problem Statement".

[i.40] IETF RFC 6105 (February 2011): "IPv6 Router Advertisement Guard".

[i.41] IETF RFC 6146 (April 2011): "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers".

[i.42] IETF RFC 6147 (April 2011): "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers".

[i.43] IETF RFC 6164 (April 2011): "Using 127-Bit IPv6 Prefixes on Inter-Router Links".

[i.44] IETF RFC 6169 (April 2011): "Security Concerns with IP Tunneling".

[i.45] IETF RFC 6192 (March 2011): "Protecting the Router Control Plane".

[i.46] IETF RFC 6221 (May 2011): "Lightweight DHCPv6 Relay Agent".

[i.47] IETF RFC 6241 (June 2011): "Network Configuration Protocol (NETCONF)".

[i.48] IETF RFC 6264 (June 2011): "An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition".

[i.49] IETF RFC 6269 (June 2011): "Issues with IP Address Sharing".

[i.50] IETF RFC 6302 (June 2011): "Logging Recommendations for Internet-Facing Servers".

[i.51] IETF RFC 6324 (August 2011): "Routing Loop Attack Using IPv6 Automatic Tunnels: Problem Statement and Proposed Mitigations".

[i.52] IETF RFC 6333 (August 2011): "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion".

[i.53] IETF RFC 6459 (January 2012): "IPv6 in 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS)".

[i.54] IETF RFC 6564 (April 2012): "A Uniform Format for IPv6 Extension Headers".

[i.55] IETF RFC 6583 (March 2012): "Operational Neighbor Discovery Problems".

[i.56] IETF RFC 6598 (April 2012): "IANA-Reserved IPv4 Prefix for Shared Address Space".

[i.57] IETF RFC 6620 (May 2012): "FCFS SAVI: First-Come, First-Served Source Address Validation Improvement for Locally Assigned IPv6 Addresses".

[i.58] IETF RFC 6666 (August 2012): "A Discard Prefix for IPv6".

[i.59] IETF RFC 6762 (February 2013): "Multicast DNS".

[i.60] IETF RFC 6763 (February 2013): "DNS-Based Service Discovery".

[i.61] IETF RFC 6810 (January 2013): "The Resource Public Key Infrastructure (RPKI) to Router Protocol".

[i.62] IETF RFC 6939 (May 2013): "Client Link-Layer Address Option in DHCPv6".

[i.63] IETF RFC 6980 (August 2013): "Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery".

[i.64] IETF RFC 7011 (September 2013): "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information".

[i.65] IETF RFC 7012 (September 2013): "Information Model for IP Flow Information Export (IPFIX)".

[i.66] IETF RFC 7039 (October 2013): "Source Address Validation Improvement (SAVI) Framework".

[i.67] IETF RFC 7045 (December 2013): "Transmission and Processing of IPv6 Extension Headers".

[i.68] IETF RFC 7050 (November 2013): "Discovery of the IPv6 Prefix Used for IPv6 Address Synthesis".

[i.69] IETF RFC 7084 (November 2013): "Basic Requirements for IPv6 Customer Edge Routers".

NOTE: Obsoletes IETF RFC 6204.

[i.70] IETF RFC 7112 (January 2014): "Implications of Oversized IPv6 Header Chains".

[i.71] IETF RFC 7113 (February 2014): "Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)".

[i.72] IETF RFC 7166 (March 2014): "Supporting Authentication Trailer for OSPFv3".

NOTE: Obsoletes IETF RFC 6506.

[i.73] IETF RFC 7381 (October 2014): "Enterprise IPv6 Deployment Guidelines".

[i.74] IETF RFC 7404 (November 2014): "Using Only Link-LocalAddressing inside an IPv6 Network".

[i.75] IETF RFC 7422 (December 2014): "Deterministic Address Mapping to Reduce Logging in Carrier-Grade NAT Deployments".

[i.76] IETF RFC 7513 (May 2015): "Source Address Validation Improvement (SAVI) Solution for DHCP".

[i.77] IETF RFC 7597 (July 2015): "Mapping of Address and Port with Encapsulation (MAP-E)".

[i.78] IETF RFC 7599 (July 2015): "Mapping of Address and Port using Translation (MAP-T)".

[i.79] IETF RFC 7610 (August 2015): "DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers".

[i.80] IETF RFC 7707 (March 2016): "Network Reconnaissance in IPv6 Networks".

NOTE: Obsoletes IETF RFC 5157.

[i.81] IETF RFC 7721 (March 2016): "Security and Privacy Considerations for IPv6 Address Generation Mechanisms".

[i.82] IETF RFC 7872 (June 2016): "Observations on the Dropping of Packets with IPv6 Extension Headers in the Real World".

[i.83] IETF RFC 7915 (June 2016): "IP/ICMP Translation Algorithm".

NOTE: Obsoletes IETF RFC 6145.

[i.84] IETF RFC 7934 (July 2016): "Host Address Availability Recommendations".

[i.85] IETF RFC 8064 (February 2017): "Recommendation on Stable IPv6 Interface Identifiers".

[i.86] IETF RFC 8190 (June 2017): "Updates to the Special-Purpose IP Address Registries".

[i.87] IETF RFC 8273 (December 2017):"Unique IPv6 Prefix per Host".

[i.88] "Mapping the Great Void - Smarter scanning for IPv6".

NOTE: Available at http://www.caida.org/workshops/isma/1202/slides/aims1202_rbarnes.pdf.

[i.89] IETF RFC 8200 (July 2017): "Internet Protocol, Version 6 (IPv6) Specification".

NOTE: Obsoletes IETF RFC 2460.

[i.90] IETF RFC 8415 (November 2018): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

NOTE: Obsoletes IETF RFC 3315.

[i.91] IEEE 802.1X™-2020: "IEEE Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control".

NOTE: Available at https://standards.ieee.org/standard/802_1X-2020.html.

[i.92] Kuhn, D. R. (2018): "A data structure for integrity protection with erasure capability. NIST Cybersecurity Whitepaper".

[i.93] Kuhn, R., Yaga, D., & Voas, J. (2019): "Rethinking distributed ledger technology". IEEE Computer, 52(2), 68-72.

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations applyː

3GPP	3rd Generation Partnership Project
AAAA	Authentication, Authorization, Accounting and Auditing
ACL	Access Control List
AFTR	Address Family Translation Router
AH	Authentication Header
AS	Autonomous System
ASIC	Application-Specific Integrated Circuit
AXFR	Authoritative Transfer
BGP	Border Gateway Protocol
CaaS	Cybersecurity as a Service
CAM	Content Addressable Memory
CE	Customer Equipment
CERT	Community Emergency Response Team
CERT	Computer Emergency Response Team Finland
CGA	CryptographicalIy Generated Address
CGN	Carrier-Grade NAT
CMDB	Configuration Management Data Base
CPE	Customer Premise Equipment
CPU	Central Processing Unit
DAD	Duplicate Address Detection
DHCP	Dynamic Host Configuration Protocol
DLT	Distributed Ledger Technology
DNS	Domain Name Service
DNSSEC	Domain Name System Security Extensions
DoS	Denial of Services
DS-Lite	Dual Stack Lite
DUID	DHCP Unique ID
ESP	Encapsulating Security Payload
EU	European Union
EUI	Extended Unique Identifier
FQDN	Fully Qualified Domain Name
GDPR	European Union General Data Protection Regulation
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation
HMAC	Hash-based Message Authentication Code
IANA	The Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ID	Identity
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IID	Interface Identifier
IP	Internet Protocol
IPAM	IP Address Management

IPfix	IP Flow Information Export
IPS	International Protective Service
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISAC	Information sharing group
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
LSN	Large Scale NAT
MAC	Media Access Control
MAP	Mapping of Address and Port
MAP-E	Mapping of Address and Port with Encapsulation
MAP-T	Mapping of Address and Port with Translation
MD5	Message Digest Algorithm Five
MIB	Management Information Base
MITM	Man-In-The-Middle
MPLS	Multi-Protocol Label Switching
MTU	Maximum Transmission Unit
NA	Neighbor Advertisement
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NCSA	National Communications Security Authority Finland
NCSC-FI	The National Cyber Security Centre Finland
ND	Neighbor Discovery
NDP	Neighbor Discovery Protocol
NESA	National Emergency Supply Agency
NETCONF	Network Configuration Protocol (NETCONF)
NOC	Network Operation Centre
NRA	National Regulatory Authority
NTP	Network Time Protocol
OECD	Organization for Economic Cooperation and Development
OS	Operating System
OSPF	Open Shortest Path First
PA	Provider Aggregatable
PE	Provider Equipment
PGW	PDN GateWay
PI	Provider Independent
PMTUD	Path MTU Detection
PPP	Point to Point Protocol
PT	Protocol Translator
RA	Router Advertisement
RADB	Routing Arbiter Database
RADIUS	Remote Authentication Dial In User Service
REC	Recommendation
RP	Router Processor
RSA	Rivest-Shamir-Adleman
RTBH	Remote Triggered Black Hole
SAINT	Systemic Analyser In Network Threats
SAVI	Source Address Validation Improvements
SeND	SEcure Neighbor Discovery
SLAAC	Stateless Address Auto Configuration
SNMP	Simple Network Management Protocol
SP	Service Provider
SSH	SecureShell
SWIFT	Society for the Worldwide Interbank Financial Telecommunication
TACACS+	Terminal Access Controller Access Control System Plus
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TLV	Type Length Value
TTL	Time To Live
TV	Television

UDP	User Datagram Protocol
ULA	Unique Local Address
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
WPA	Wi-Fi Protected Address

4 Generic IPv6 Security Considerations

4.1 Addressing Architecture

4.1.1 Introduction

IPv6 address allocations and overall architecture are an important part of securing IPv6. Initial designs, even if intended to be temporary, tend to last much longer than expected. Although initially IPv6 was thought to make renumbering easy, in practice, it may be extremely difficult to renumber without a good IP Addresses Management (IPAM) system.

Once an address allocation has been assigned, there should be some thought given to an overall address allocation plan. With the abundance of address space available, an address allocation may be structured around services along with geographic locations, which then can be a basis for more structured security policies to permit or deny services between geographic regions.

A common question is whether companies should use Provider Independent (PI) vs. Provider Aggregatable (PA) space (IETF RFC 7381 [i.73]), but from a security perspective there is little difference. However, one aspect to keep in mind is who has administrative ownership of the address space and who is technically responsible if/when there is a need to enforce restrictions on routability of the space due to malicious criminal activity. Using PA space exposes the organization to a renumbering of the complete network including security policies (based on ACL), audit system, etc., in short a complex task which could lead to some temporary security risk if done for a large network and without automation; hence, for large networks, PI space should be preferred even if it comes with additional complexities (for example BGP routing) and duties (adding a route6 object in the Regional Internet Registry database).

In IETF RFC 7934 [i.84], it is recommended that IPv6 network deployments provide multiple IPv6 addresses from each prefix to general-purpose hosts and it specifically does not recommend to limit a host to only one IPv6 address per prefix. It also recommends that the network give the host the ability to use new addresses without requiring explicit requests (for example by using SLAAC).

4.1.2 Statically Configured Addresses

When considering how to assign statically configured addresses it is necessary to take into consideration the effectiveness of perimeter security in a given environment. There is a trade-off between ease of operation (where some portions of the IPv6 address could be easily recognizable for operational debugging and troubleshooting) versus the risk of trivial scanning used for reconnaissance. SCANNING [i.88] shows that there are scientifically based mechanisms that make scanning for IPv6 reachable nodes more realizable than expected; see also IETF RFC 7707 [i.80]. The use of well-known (such as ff02::1 for all link-local nodes) or the use of commonly repeated addresses could make it easy to figure out which devices are name servers, routers or other critical devices; even a simple trace route will expose most of the routers on a path. There are many scanning techniques and more to come possible, hence, operators should never rely on the 'impossible to find because my address is random' paradigm.

While in some environments obfuscating addresses could be considered an added benefit; it does not preclude that perimeter rules are actively enforced and that statically configured addresses follow some logical allocation scheme for ease of operation (as simplicity always helps security). Typical deployments will have a mix of static and non-static addresses.

4.1.3 Use of ULAs

Unique Local Addresses (ULAs) (IETF RFC 4193 [i.20]) are intended for scenarios where systems are not globally reachable, despite formally having global scope. ULA looks similar to IETF RFC 1918 [i.8] addresses but have different use cases. One use of ULA is described in IETF RFC 4864 [i.32] and some considerations on using ULA are described in IETF draft-ietf-v6ops-ula-usage-considerations [i.5].