PKI & RadSec

End-Entity Deployment Guidelines

Source: WBA
Author(s): WBA Roaming Evolution
Issue date: April 2021
Version: 1.2.0
Document status: Final

WIRELESS BROADBAND ALLIANCE
DRIVING NEXT WIRELESS EXPERIENCE

ABOUT THE WIRELESS BROADBAND ALLIANCE

Wireless Broadband Alliance (WBA) is the global organization that connects people with the latest Wi-Fi initiatives. Founded in 2003, the vision of the Wireless Broadband Alliance (WBA) is to drive seamless, interoperable service experiences via Wi-Fi within the global wireless ecosystem. WBA's mission is to enable collaboration between service providers, technology companies, cities, regulators and organizations to achieve that vision. WBA's membership is comprised of major operators, identity providers and leading technology companies across the Wi-Fi ecosystem with the shared vision.

WBA undertakes programs and activities to address business and technical issues, as well as opportunities, for member companies. WBA work areas include standards development, industry guidelines, trials, certification and advocacy. Its key programs include NextGen Wi-Fi, OpenRoaming, 5G, IoT, Testing & Interoperability and Policy & Regulatory Affairs, with member-led Work Groups dedicated to resolving standards and technical issues to promote end-to-end services and accelerate business opportunities.

The **WBA Board** includes AT&T, Boingo Wireless, Broadcom, BT, Cisco Systems, Comcast, Deutsche Telekom AG, GlobalReach Technology, Google, Intel, Reliance Jio, SK Telecom and Viasat.

For the complete list of current WBA members, **click here**.

Follow Wireless Broadband Alliance:

www.twitter.com/wballiance

http://www.facebook.com/WirelessBroadbandAlliance

https://www.linkedin.com/company/wireless-broadband-alliance

CONFIDENTIALITY

Privileged/confidential information may be contained in this document and any files attached in it ('WBA Documentation').

Only WBA member companies who have signed the new WBA IPR Policy (Located at: **http://extranet.wballiance.com/apps/org/workgroup/inf_cen/document.php?document_id=2125**) and are the intended recipient are entitled to receive, review or comment on this WBA Documentation.

If you are not the intended recipient (or have received this WBA Documentation in error), please notify the sender and WBA (**pmo@wballiance.com**) immediately and delete this WBA Documentation. Any unauthorized copying, disclosure, use or distribution of this WBA Documentation is strictly forbidden.

UNDERTAKINGS AND LIMITATION OF LIABILITY

This Document and all the information contained in this Document is provided on an 'as is' basis without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for particular purpose, or non-infringement.

In addition, the WBA (and all other organizations who may have contributed to this document) makes no representations or warranties about the accuracy, completeness, or suitability for any purpose of the information. The information may contain technical inaccuracies or typographical errors. All liabilities of the WBA (and all other organizations who may have contributed to this document) howsoever arising for any such inaccuracies, errors, incompleteness, suitability, merchantability, fitness and non-infringement are expressly excluded to the fullest extent permitted by law. None of the contributors make any representation or offer to license any of their intellectual property rights to the other, or to any third party. Nothing in this information or communication shall be relied on by any recipient.

The WBA also disclaims any responsibility for identifying the existence of or for evaluating the applicability of any claimed copyrights, patents, patent applications, or other intellectual property rights, and will take no position on the validity or scope of any such rights. The WBA takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any effort to identify any such rights.

Neither the WBA nor any of the other organizations who may have contributed to this document will be liable for loss or damage arising out of or in connection with the use of this information. This is a comprehensive limitation of liability that applies to all damages of any kind, including (without limitation) compensatory, direct, indirect or consequential damages, loss of data, income or profit, loss of or damage to property and claims of third-parties.

TABLE OF CONTENTS

FIGURES

1 Introduction

With the growth of Wi-Fi interoperability and Wi-Fi roaming services, more service providers of Wi-Fi radio, network-access services and identify providers see the value in interworking together, and through intermediaries, to enhance the breadth and depth of the Wi-Fi user-experience.

RadSec secure connection, under the WBA Public Key Infrastructure (PKI), provides a highly scalable means to allow these entities to interwork for the benefit of their end-users.

This document focuses on providing information and guidelines for End-Entities (organisations with Wi-Fi coverage and/or subscribers) who wish to deploy WBA's interoperable RadSec service. The WBA believes that this single document provides the source to encourage End-Entities to adopt WBA PKI RadSec to expand their Wi-Fi business.

2 Purpose

The purpose of this guide is to inform prospective End-Entities (Wi-Fi network providers and/or Wi-Fi User Identity providers) on how RadSec can help their interworking business, and to offer recommendations and guidelines on using WBA PKI RadSec.

2.1 General Description

This document is focused on providing information and guidelines to those service-providers who are End-Entities in the WBA Wi-Fi roaming ecosystem. That is, End-Entities who have Wi-Fi network coverage to offer to the WBA ecosystem and who as a consequence are looking to deploy RadSec client functionality, and/or End-Entities who have wireless subscription end-user identities and who as a consequence are looking to deploy RadSec server functionality.

This guide contains deployment guidelines for implementing RADIUS interconnections to/from those RADIUS clients/servers using RadSec connectivity which is secured using the Wireless Broadband Alliance (WBA) Public Key Infrastructure (PKI).

These guidelines are also intended to help End-Entity planners and systems engineers, ensuring that RadSec installations go smoothly and efficiently. Adherence to the practices defined will also allow End-Entities to adopt a standardized configuration approach and allow them to securely interwork with other entities, including WBA PKI Registration Authority agents, Interconnectivity providers, and data-clearing/financial-settlement providers.

3 WBA PKI Certificate Policy Overview

The WBA PKI defines the use of digital certificates to enable the use of public-key encryption for protecting RADIUS messages signaled across the WBA's Wireless Roaming Intermediary eXchange (WRIX). Unlike conventional bi-lateral roaming where only two parties are involved in key exchange, a PKI requires various roles to be performed which are often implemented by different participants, including the End-Entities that support the RADIUS client/server functionality, but also the different Certificate/Registration Authorities that are essential to the operation of the PKI.

The Certificate Policy is used to define the roles of all participants in the PKI. The WBA's PKI Certificate Policy is a public document and is available to view **HERE**.

In addition, the WBA PKI certificates include the same link, enabling all parties that are relying on the security delivered using the WBA PKI to understand the policies used across the PKI.

4 RadSec Definition and Benefits

RadSec provides a means of securing the communication between two RADIUS peers. The Internet Engineering Task Force (IETF) has defined both a Transport Layer Security (TLS) and a Datagram Transport Layer Security (DTLS) approach for securing RadSec connections.

The WBA has adopted TLS for securing RadSec connections signaled across WBA compliant Wireless Roaming Intermediary eXchange (WRIX) participants. The broad idea is that, when an End-Entity supports WBA RadSec connectivity, they can interoperate with a

very broad range of peer entities, who also enjoy interconnection, clearing, settlement and Wi-Fi location services.

The WBA RadSec framework and its benefits are described in detail in the **WBA PKI & RadSec Operator Deployment Guidelines** document. RadSec lends itself to lightweight and efficient End-Entity sign-up and connection to the WBA interworking ecosystem.

From an End-Entity point of view, the important concepts and benefits of the WBA PKI RadSec framework are as follows:

- **Interoperability**: with a WBA PKI certificate provided through a WBA RA Agent, an End-Entity should be able to securely connect for RADIUS (authentication, authorization and usage accounting) with any and all RadSec services of counter-parties in the WBA ecosystem.
- **End-Entity Identification**: The WBA PKI Framework ensures all entities are properly identified using the **WBA Unique Organization Identifier: WBAID** (described in **WBA WRIX Umbrella** document), aiding operational robustness.
- **Scalability**: The WBA PKI Framework defines a hierarchical approach to certificate management and identity management. The WBA RadSec PKI defines the use of Agents, including the WBA PKI Registration Authority that can help the End-Entity to obtain a suitably signed WBA PKI X.509 certificate. From an Identity Management perspective, End-entities can get WBAID identifiers for their service, either by:
    - Becoming members of the WBA, and being assigned a WBAID (Primary Member ID), or;
    - Engaging with a WBA Authorized Partner, as an Agent, to sponsor and assign them a WBAID (SubID) in the form of <“AgentAssignedSUBID”>.<”the Agent’s WBAID”>. In this manner, End-Entities need not be WBA Members, but can use Agency WBA Members to take advantage of WBA ecosystem connectivity, clearing, location-management, etc.

When the End-Entity installs the WBA PKI certificate, there is the ability to establish a secure connection with other RadSec peer or hub entities (like WRIX-i connectivity providers, etc.) to allow Wi-Fi AAA service in the WBA ecosystem.

5 RadSec Hierarchy Roles and Deployment Guidance

The key aspect of RadSec is the use of a TLS connection over which the RADIUS messages are exchanged. TLS is supported through the mutual exchange of trusted certificates. To enable the trust of these certificate, the WBA has created the WBA PKI Certificate Policy [1]. Defined in the Certificate Policy are the hierarchical roles of different levels within the trusted certificate chain. Figure 1 shows the different levels within the PKI hierarchy:

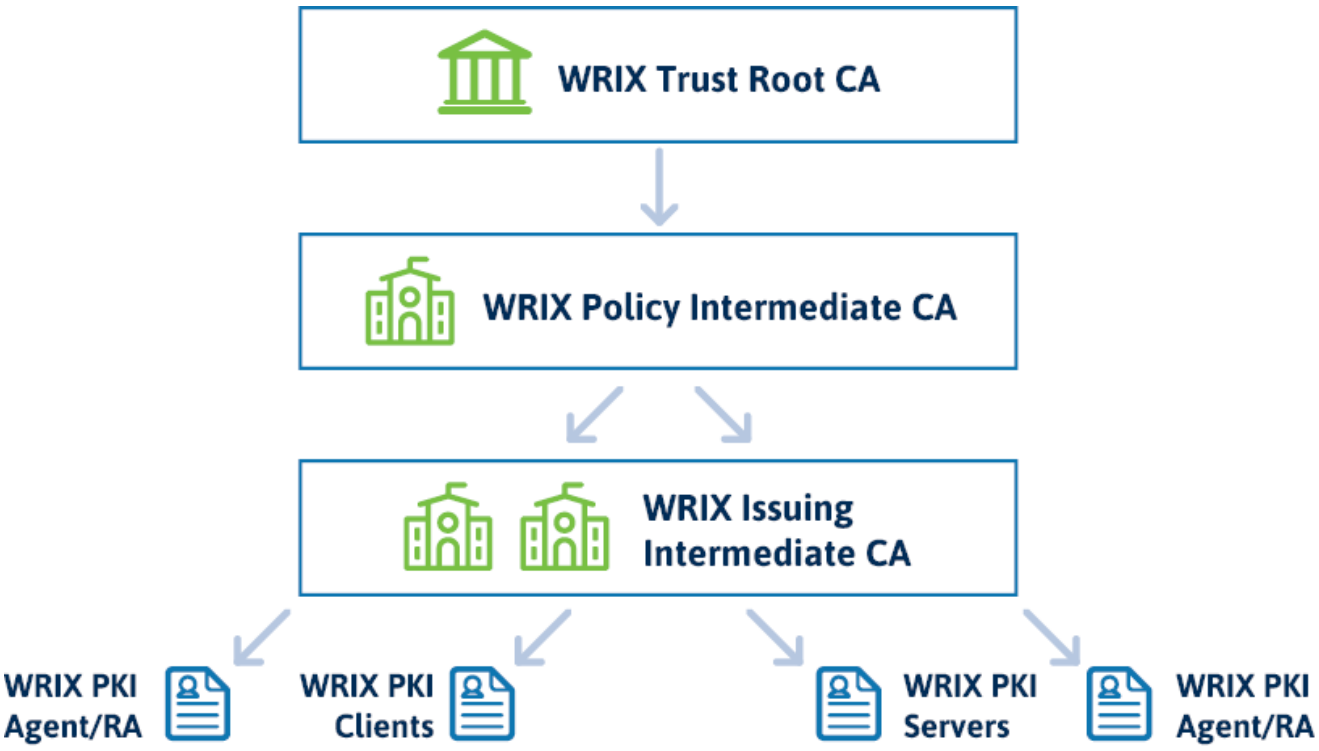

Figure 1 WBA PKI Hierarchy

The hierarchy starts at the top with the WRIX Trusted Root Certificate Authority (CA) which hosts the root certificate. The WRIX Trust Root CA is responsible for the issuance of certificates to the WRIX Policy Intermediate CAs. The WRIX Policy Intermediate CA is responsible for issuance of certificates to the WRIX Issuing Intermediate CAs. The next level is the WRIX Issuing Intermediate CA which is responsible for issuance of certificates for the WRIX Registration Authority (RA) Agents (referred to as the WRIX Agents) and End-Entities. The WRIX Agents are responsible for verifying End-Entities and submitting requests to the WRIX Issuing Intermediate CA for End-Entity certificates. The WRIX Issuing Intermediate CA

will then issue the End-Entity certificates directly or through the Registration Authority (RA) Agent. The WRIX PKI clients and servers are the End-Entities that interconnect using RadSec for the exchange of RADIUS messages.

5.1 WBA WRIX End Entity in the RadSec Framework

The WBA WRIX documentation [3] covers the recommended practices for interworking, including interworking involving WBA PKI RadSec.

The WBA WRIX-n [4] (with technical interconnection recommended practices, specifically for End-Entities) and WRIX-i [5] documents (with technical interoperability recommendations) cover the specifications of RadSec connections.

RadSec supports automated processes to authenticate and trust PKI-secured associations to allow secured RADIUS message exchange between End-Entities. This allows End-Entities to interoperate with a very high scale of counterparties. It also enables automated management of these associations. The WBA WRIX technical specification documentation and associated guideline information describe how WBA RadSec works with PKI certification.

This scalability enables WBA OpenRoaming™ [6]. By following WBA WRIX practices, in combining key enablers including the WBAID (to unambiguously identify the End-Entity to the WBA OpenRoaming market), the End-Entity can use RadSec to efficiently enter the WBA OpenRoaming market.

5.2 WBA WRIX Authorized Agent

The WBA WRIX Authorized Agent is an organization that performs the service of providing End-Entities with WRIX End-Entity certificates and/or WBAIDs. The Agent may also be referred to as a ‘Registration Authority’ when preforming certificate issuance.

The WRIX Agent, in the role of the Registration Authority, validates and approves certificate requests. The WRIX Agent collects and verifies the WRIX End-Entity’s identity and the information that is to be entered in the public key certificate. The WRIX Agent interacts with

the Issuing Intermediate CA to enter approved WRIX End-Entity certificate request information.

In addition to the Registration Authority functions, the WRIX Agent may also provide WBAIDs to WRIX End-Entities. Refer to the Operators Deployment Guide [2] and the WRIX framework [3] documents for more details on the allocation of WBAID.

5.3 WRIX Agents and WRIX End-Entity Interactions

The WRIX Agent as a Registration Authority of WBA's PKI is responsible for accepting requests for digital certificates directly from WRIX End-Entities. The exact details of the engagement between the WRIX End-Entity and the WRIX Agent is not defined by the WBA Certificate Policy, but the WRIX Agent must publish its procedures in a practice statement. This means that a WRIX End-Entity may wish to engage with several potential WRIX Agents to understand their exact procedures, e.g., whether interaction is online or offline, what automated services are supported, etc.

Irrespective of how they are delivered, there are a set of key tasks that are required of the interaction between WRIX Agent and WRIX End-Entity. These include:

1. The identification and authentication of entities who wish to apply for a WBA PKI certificate
2. The procedures that enable authenticated End-Entities to submit their certificate applications
3. The validation of the information that is to be included in the subject field of the End-Entities certificate
4. The approval of certificate applications, or rejection if the above validation fails
5. The procedures that enable an End-Entity to trigger the revocation of an issued certificate
6. The procedures that enable an End-Entity to renew a digital certificate

The procedure of how an issued certificate is delivered to the End-Entity is not defined by the WBA's Certificate Policy and is instead defined by the WRIX Agent. Options include having an issued certificate delivered directly to the End-Entity from the Issuing I-CA or delivered via the WRIX Agent.

5.4 WBAID and WBA WRIX PKI

Before an End-Entity may obtain a certificate for WBA RadSec, the End-Entity is required to have a WBAID. The WBAID may be obtained from the WBA PKI Agent processing the certificate request if the End-Entity needs one. The WBA PKI Agent ensures that the End-Entity has a valid WBAID if one is provided. The signed certificate will be identifiable with the End-Entity's WBAID.

5.5 Implementation of RadSec

As described in IETF RFCs and in the WBA framework, RadSec connections are bilateral by nature. They use a mutually authenticated form of TLS, where the RadSec client End-Entity is authenticated at the same time as the RadSec server End-Entity is authenticated. Both certificates are checked as being in a Root-signed chain of trust established by the WBA PKI Policy's Root Certificate Authority. The validity of the X.509 certificates and their signatures within the root-signed PKI are a key part of the security of the deployment.

Before publishing the WBA PKI Certificate Policy, the WBA made an evaluation of the capabilities of several different RadSec implementations (both commercial and open source). This analysis demonstrated that several different implementations were available that met the requirements of the WBA.

Note: the use of TLS for protecting the transport of the RADIUS messages is separate and distinct from the possible use of TLS as part of any EAP method exchange. The WBA's Certificate Profile currently defines the use of the WBA PKI for protecting network-to-network

interfaces between entities involved with delivering the functionality to support WRIX and is not intended to be used as part of any EAP method.

5.6 RadSec Server and Client Selection

The RadSec ecosystem involves a two-party TLS connection that consists of a RadSec server and a RadSec client. In implementing RadSec, an End-Entity needs to determine which, if not both, roles they want to operate. This section reviews the purpose of each role to help the End-Entity determine the role they need to act in or if they need to act as both roles.

At the start of a RadSec exchange, the connection is initiated by a client to a server. Depending on the RadSec implementation, the RadSec connection can be initiated upon the client startup and maintained over time or can be initiated when a RADIUS exchange is initiated.

Since PKI certificates are involved, certificates are needed for both the server and client. There are three WBA PKI certificate types:

- a client certificate, where the Extended Key Usage in the issued certificate indicates it is to be used for TLS Client Authentication;
- a server certificate, where the Extended Key Usage in the issued certificate indicates it is to be used for TLS Server Authentication; and
- a server/client certificate, where the Extended Key Usage in the issued certificate indicates it is to be used for both TLS Client and TLS Server Authentication.

This allows an End-Entity to operate in the roles of server, client, or both with only a single certificate.

5.7 RadSec Server

The role of the RadSec Server is hosted by an End-Entity that will be receiving RadSec TLS connection request from a RadSec Client and responding to the RADIUS exchange. End-Entities that have this role are Home Service Providers (HSP) that authenticate users, Hub

Providers, and Aggregators. In this role, the RadSec PKI certificate Extended Key Usage must permit use for TLS Server Authentication.

5.8 RadSec Client

The role of the RadSec Client is hosted on an End-Entity that initiates the RadSec TLS connection and the RADIUS exchange. End-Entities that have this role are Visited Network Providers (VNP), HUB Providers, and Aggregators. In this role, the RadSec PKI certificate Extended Key Usage must permit use for TLS Client Authentication.

5.9 RadSec Server/Client

In the cases where the End-Entity serves as a Visited Network Provider and a Home Service Provider (HSP), the roles of RadSec Server and Client may be combined depending on the flow of the RADIUS exchange.

In this role, it's recommended that a RadSec PKI server/client certificate be used; however, at the discretion of the End-Entity separate server/client and client RadSec PKI certificates may be used.

An example of this: in cases where the End-Entity makes use of two different IP addresses or DNS names depending on the direction of the RADIUS message flow. Specifically, this is when the RADIUS initiated traffic is seen by the RadSec Server for one IP address or DNS resolved IP address and the receiving RADIUS traffic is sent to the RadSec Client on a different IP address or DNS resolved IP address. The reason for this is that certificates may contain either the IP address or DNS name of the server to allow for matching of the certificate to the server that offers the certificate.

5.10 Testing of RadSec Connection

To help ensure the functionality of the RadSec connection, testing of the connection with each peer is recommended. This testing should include both positive and negative test cases

to ensure the proper function of the TLS connection to reduce the risk of an invalid connection.

Positive testing should include the successful setup of the TLS connection and exchange of the various RADIUS messages using for authentication and accounting (if applicable). This can be completed by monitoring the connection and performing a test RADIUS exchange.

Negative testing should include areas where the RadSec connection should not be completed. These include the following:

- Invalid peering certificate
- Expired peering certificate
- Untrusted certificate
- Revoked certificate
- A certificate that is not yet valid

Some of the above conditions can be tested through settings of the server, such as not having the Trusted Root CA installed, or overriding the time settings on the server. Other conditions will require special certificates. The special certificates could be self-generated or could be requested through the WBA WRIX Agent.

5.11 Dynamic Discovery of RadSec Endpoints

Operators of RadSec server functionality may optionally decide to support dynamic discovery of their RadSec endpoints using DNS. If an operator intends to support dynamic discovery, then they shall ensure that the NAIrealms for those realms for which they are authoritative are included in their WBA PKI certificate in the Subject Alt Name field.

The approach used by the WRIX Agent for verifying that the WRIX End Entity is authoritative for a particular REALM shall be described in its RA practice statement.

An operator deciding to support optional dynamic discovery shall configure their DNS entry to include their NAPTR, SRV and A resource records according to RFC 7585. The NAPTR record shall include the "aaa+auth:radius.tls.tcp" “” _radiustls._tcp.<realm> entry which

signals the supported traffic type (aaa+auth) and protocol (radius.tls.tcp) as well as a pointer to the service record (_radiustls._tcp.<realm>).

There are procedures that need to be supported by RadSec endpoints that support the dynamic discovery of a RadSec endpoint. If a RadSec client that supports dynamic discovery receives a server certificate which does not include a subjectAltName:dNSName which matches the realm in the initiator, the client shall reject the authentication and should log the event.

When supported, the ordering of how to use the dynamic discovery of a signaling endpoint should be performed in the following order:

1. The RadSec client first compares a particular user's realm in the Access-Request with its list of manually configured RadSec Servers (that are static Routing Table entries);
2. If the realm doesn't match a static routing entry, the RadSec client performs a NAPTR query for a server in a particular realm;
3. If no NAPTR records are found, the RadSec client uses a static "route of last resort" to identify the RadSec peer.

6 WBA WRIX PKI Certificate Life Cycle

6.1 Requesting

The WBA Certificate Policy places requirements on the PKI participants, including placing requirements on Certificate and Registration Authorities that enable the scalable operation of the PKI system.

As the WBA PKI Agent has the direct relationship with the End-Entity, it plays a key role in terms of collecting and verifying information related to the End-Entity. The WBA PKI Agent's obligations include:

- confirming the identity of the Certificate Applicant (valid constituent of the WRIX End-Entity);

- collecting and verifying from each WRIX End-Entity, the information that is to be entered in the public key Certificate; and
- confirming the End-Entity is in possession of a private key

The WBA PKI Agent uses this information to assist in either approving or denying the Certificate Application from the End-Entity. The WBA does not describe the exact procedures for performing these operations. However, the WBA PKI Agent is responsible for describing the steps involved in all processes related to PKI operation in its practice statement.

Steps may include the End-Entity registering with a particular WBA PKI Agent, the agreement of the subject DN to be included in the certificate, the allocation of a subordinate identity under the WBAID namespace of a primary WBA member or checking the validity of an issued primary member ID.

Other steps may be dependent on the particular services being delivered by the agent to the End-Entity. For example, if the End-Entity expects to receive payment for Wi-Fi service, then the steps may include sharing of information related to the configuration of the End-Entity's RADIUS clients and Agent's RADIUS servers, e.g., to ensure that the agent is able to generate the appropriate records used in data clearing and financial settlement. In other cases, if the End-Entity corresponds to a HSP and is expecting to have to make payment for Wi-Fi services delivered by different VNPs, then additional steps will likely include exchanging financial information to enable credit checking procedures to be completed.

After all checks have been successfully completed, the Agent will trigger the issuance of a certificate to the End-Entity. If the Agent operates an Issuing Certificate Authority, then the Agent will also be responsible for issuing the certificate. If the Agent operates a Registration Authority, then the Agent will forward the Certificate Signing Request to its nominated Issuing Certificate Authority. In either approach, the Issuing Certificate Authority is required to share the subject DN information included in the certificate with the WBA.

In summary, the steps and criteria that End-Entities undergo with WRIX PKI Agents will be defined and agreed between them: the overall goal of the WBA PKI Agent being that, once certified, the End-Entity will be able to discharge their obligations to the rest of the WBA

ecosystem, specifically ensuring that the End-Entity complies to the WBA WRIX RADIUS and PKI RadSec policies in their implementation.

6.2 Renewal

All WRIX End-Entity public key certificates have a finite lifespan. The WBA PKI policy permits End-Entity certificates to be issued for up to 3 years, but an Issuing Certificate Authority may decide to issue certificates for a shorter validity period. This means that the WBA PKI certificates need to be replaced before the end of their life to avoid service disruption.

Once again, the WBA does not describe the exact procedures for performing certificate renewal. However, the WBA PKI Certificate Policy requires that the renewed certificate does not re-use an existing key pair, and hence as a minimum, the WBA PKI Agent is responsible for confirming the End-Entity is in possession of a new key pair.

6.3 Revocation

The WBA PKI Certificate Policy places requirements on the revocation of issued certificates. However, the WBA does not describe the exact procedures between the WBA PKI Agent and the End-Entity for triggering certificate revocation.

The WBA PKI Agent is responsible for ensuring that information in issued certificates remains valid. For example, if an End-Entity ceases trading or terminates its relationship with the WBA PKI Agent, the WBA PKI Agent is responsible for triggering the revocation of the End-Entity's issued certificates.

The End-Entity also has responsibilities for triggering the revocation of issued certificates. For example, if the End-Entity becomes aware that a private key has been compromised, then it shall trigger the revocation of the associated certificate. If the End-Entity changes its organization name, then all certificates issued to the previous organization shall be revoked. Finally, if the End-Entity disposes of equipment that has embedded a WBA PKI certificate, then the End-Entity is responsible for triggering the revocation of the certificate.

In the event the WBA detects the improper use of certificates e.g. usage contravenes the WBA PKI Certificate Policy, the WBA reserves the right to trigger the revocation of an End-Entity certificate.

7 Conclusion

Launch and use of Public Key Infrastructure (PKI) is the stepping-stone towards building a “chain of trust” for the WBA ecosystem, aiming to simplify and automate security to enable scalable roaming relations. The PKI not only allows clients/servers to verify who they say they are; it also enables networks to allow those clients/servers access once authenticated and approved. This improves the overall security, scalability and interoperability of Wi-Fi networks and connected devices.

As the PKI Policy Authority, WBA is committed to govern this ecosystem in alignment with the policies defined on the latest PKI Certificate Policy, as approved by the membership.

To guarantee enhanced partner discovery and long tail opportunities, along with an evolved roaming architecture to bridge the divide between federations (integrated signaling, reporting, policy), it is fundamental that guidelines are followed, and relations are maintained based on industry defined best practices.

The end game of these guidelines is therefore to serve the stakeholders part of the PKI Certificate Policy, that depending on their hierarchy role, will have an active part in maintaining the harmony of the ecosystem, flawless operation, and its overall success.

7.1 Guidelines Maintenance Process

WBA is committed to maintain these guidelines aligned with latest developments, and as a result, industry wide feedback and participation is welcome.

By nature, it is expected these guidelines will evolve as the technology is adopted, and deployments scale.

The project leadership and editorial team, in conjunction with WBA Program Management Office, guarantee all documentation update requests to reflect any of the latest assumptions are considered. Updates follow regular technical activities approval process.

For more information or learn how to engage, please contact the WBA at:

- **pmo@wballiance.com**
- **contactus@wballiance.com**

REFERENCES

[1] **WBA PKI Certificate Policy – WBA**

[2] **PKI RadSec Operator Deployment Guidelines**

[3] **WRIX Umbrella Document - WBA**

[4] **WRIX-n – Network**

[5] **WRIX-i - Interconnect**

[6] **WBA OpenRoaming™ Standard**

ACRONYMS AND ABBREVIATIONS

ACRONYM / ABBREVIATION	DEFINITION
AAA	Authentication, Authorization and Accounting
CA	Certificate Authority
CP	Certificate Policy
DTLS	Datagram Transport Layer Security
HSP	Home Service Provider
I-CA	Intermediate Certificate Authority
IETF	Internet Engineering Task Force
Issuing I-CA	Issuing Intermediate Certificate Authority
PA	Policy Authority
PKI	Public Key Infrastructure
RA	Registration Authority
TLS	Transport Layer Security
VNP	Visited Network Provider
WBA	Wireless Broadband Alliance
WBAID	WBA Identifier
WGC	Wireless Global Congress
WRIX	Wireless Roaming Intermediary eXchange

Annex A: Informative example of CSR generation

This annex provides examples of how to use OpenSSL Command Line Utility to generate a Certificate Signing Request (CSR) to use with a WBA PKI Issuing I-CA for issuing an End-Entity certificate. The OpenSSL utility may need to be downloaded and/or installed on the system before following the example below.

The ECC private key, file is named secure_private_key.pem in the example below, should be securely stored and protected. The private key should not be shared. Refer to the WBA PKI CP with regards to private key protection.

A.1 CSR Configuration File Format

This informative example is based on a configuration file, in these examples named "config.cfg".

A.1.1 Example End-Entity Client Configuration File

Create the config.cfg file with the following contents:

```
[req]
distinguished_name = req_distinguished_name
prompt = no

[req_distinguished_name]
# The organization two letter country code (C)
C = ZZ
# The organization (O) exact documented name
O = ABC Company, Inc
# The organizational unit (OU) is controlled by the CA and cannot be changed
OU= WBA:WRIX End-Entity
# The unique common name (CN) for the certificate (i.e. domain name like serv1.abc-company.com or any unique name such as Server1)
CN = endpoint.abc-company.com
# The WBA Unique Identification for the organization
UID=ABC Company:ZZ
```

A.1.2 Example End-Entity Server or Client/Server Configuration File

Create the config.cfg file with the following contents:

```
[req]
distinguished_name = req_distinguished_name
req_extensions     = v3_req
x509_extensions    = v3_req
prompt = no

[req_distinguished_name]
# The organization two letter country code (C)
C = ZZ
# The organization (O) exact documented name
O = ABC Company, Inc
# The organizational unit (OU) is controlled by the RA/CA and cannot be changed
OU= WBA:WRIX End-Entity
# The unique common name (CN) for the certificate (i.e. domain name like serv1.abc-company.com or any unique name such as Server1)
CN = endpoint.abc-company.com
# The WBA Unique Identification for the organization
UID=ABC Company:ZZ

[v3_req]
# WBA Server certificates require at least one subjectAltName DNS, multiple entries and wildcards are allowed
subjectAltName       = @alt_names

[alt_names]
# each DNS will be the allowed/accepted RadSec realms
DNS.1   = *.abcompany.com
DNS.2   = some.realm.com
DNS.3   = *.roam.jp
```

A.2 Generation of ECC private key and CSR file

Generate the ECC private key.

- The -out filename parameter can be changed to anything.

  openssl ecparam -name secp384r1 -genkey -out secure_private_key.pem

Make the certificate signing request (CSR) using the config file and private key.

- The -out filename parameter can be changed to anything.
- The -key filename parameter should match the filename from the previous step.
- The -config parameter is the filename of the configuration parameters from the previous section.

  openssl req -new -sha256 -config config.cfg -key secure_private_key.pem -out company_wba_csr.pem

CSR can be checked and the information validated with the following command.

- The -in filename parameter will be the filename of the csr file created in the previous step.

  openssl req -text -noout -in company_wba_csr.pem

DOCUMENT HISTORY

VERSION	REVISION DATE	REVISED BY	DESCRIPTION OF CHANGE
1.0.0	August, 2020	Scott Reaves (Single Digits)	First published version
1.1.0	October, 2020	Scott Reaves (Single Digits)	Added certificate annex
1.2.0	April, 2021	Shawn Moss (Kyrio)	Updated certificate annex