NOKIA

Demo

About Nokia

Nokia is a global leader in the technologies that connect people and things. Powered by the innovation of Nokia Bell Labs and Nokia Technologies, the company is at the forefront of creating and licensing the technologies that are increasingly at the heart of our connected lives.
With state-of-the-art software, hardware and services for any type of network, Nokia is uniquely positioned to help communications service providers, governments, and large enterprises deliver on the promise of 5G, the Cloud and the Internet of Things.
www.nokia.com

NOKIA

Table of contents

1. Introduction

The Nokia Authentication, Authorization and Accounting (AAA) is the server of choice for major service providers, ISPs and Enterprises due to its proven performance and its flexible, extensible architecture built on Java™-based programming language. Nokia AAA provides the tools needed to support the technologies and services of today as well as of tomorrow.

The Nokia AUthentication Service (AUS) is the 5G Cloud Native Blueprint solution which is built from the Nokia AAA Core Software and delivered as a Cloud Native Micro Service. This solution is designed and delivered specifically to support the 3GPPP 5G requirements for Authentication Service Function (AUSF).

Details of this solution are outlined in the Blueprint section of this document.

The Nokia AAA server offers the most extensive set of Nokia AAA features available today for wireline, broadband, and wireless networks. Extensive support for IETF RFCs (AAA, RADIUS, Diameter, TACACS and EAP), TIA (IS-835), 3GPP, and 3GPP2 standard support means that the Nokia AAA server is equipped to support a wide array of access technologies including: CDMA, GSM/GPRS, UMTS, Broadband, GPON, LTE, 5G, WiFi, WiFi Offload, VoWiFi, Femto, and VPN/tunnelling.

AAA provides the following benefits:

- Increased flexibility and control
- Scalability
- Standardized authentication methods (RADIUS, TACACS+, Diameter, HTPP2)

2. Solution Overview

The AAA consists of three key components: a policy engine (Nokia AAA Front End), a Session State Repository, and a JAVA based element management application referred to as the Server Management Tool (SMT). The product's architecture is extremely flexible which allows for all three functions to be deployed on a single machine or distributed across multiple machines. An example of a distributed configuration is shown in the figure below.

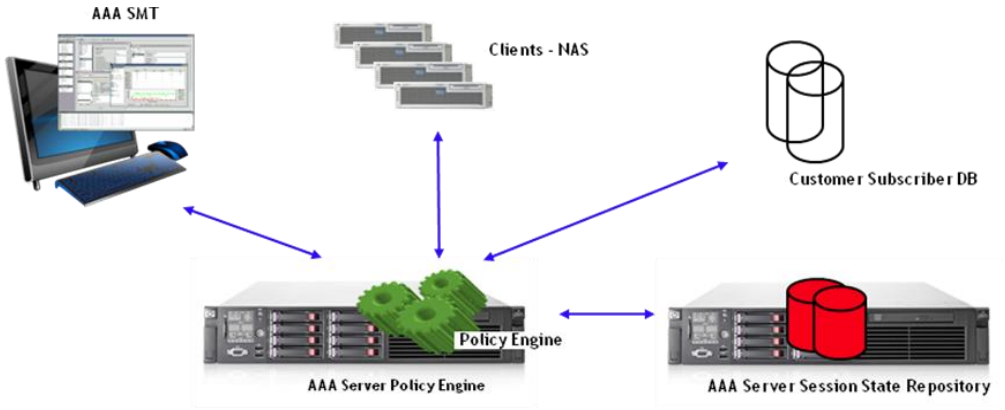

Figure 1

The Nokia AAA has been designed from the ground up to be one of the most efficient AAA servers on the market. The product is optimized to take full advantage of today's multi-core and multi-threaded CPUs. This allows it to scale across a wide variety of hardware platforms and makes it possible for service provider to get the most out of their hardware investment. Adding additional Nokia AAA capacity/throughput is as simple as deploying a new server instance or upgrading the existing platform. This makes it possible for the product to scale to meet the needs of the world's largest service providers.

The Nokia AAA has been designed with an emphasis on performance.

The Intelligent request queue management makes it possible for the server to: detect and filter out duplicate requests which help to reduce the load on the server as well as backend systems, cache responses for retransmission when needed, and graceful handling of overload situations by focusing on requests with the highest probability of success.
The PolicyFlow language allows for defining highly customized policies that only perform the steps explicitly required in making a policy decision. Queries to backend systems can be load balanced to improve performance.
The Universal State Servers allows to monitor and control the current active sessions.

All of these capabilities result in an extremely efficient product capable of processing thousand of authentication and/or accounting transactions per second on commodity hardware platforms. Additional Nokia AAA servers can be deployed as transaction growth occurs. The performance of the product has been proven in some of the world's largest service providers where it has scaled to support millions of subscribers.

Nokia AAA can be deployed in a central data center or in a distributed manner to provide geographic redundancy. Nokia AAA's interfaces (LDAP, HTTP Get/Post, and JDBC SQL) to backend systems support a variety of error detection and retry strategies. This is vital to increasing the overall availability of a customer's Nokia AAA solution.

In summary, the Nokia AAA solution can be characterized as:

Customizable – A high performance, JAVA based architecture allows customers to completely customize Nokia AAA to support unique authorization, authentication and accounting policies as well as unique integration requirements.
Scalable – Advanced use of multi-threaded technology allows Nokia AAA to achieve extremely high transaction rates on relatively streamline servers with benchmarking over 10K transactions per sec.
Reliable – With over 10 years of field history, Nokia AAA is a hardened highly reliable network component that is able to operate and consistently deliver Nokia AAA services in the most demanding environments.

2.1 Core Capabilities

2.1.1 Nokia AAA Session State Repository

The Nokia AAA Session State Repository is an in memory repository that keeps track of all active sessions. The active session records stored in the repository are triggered and updated by events like:

- RADIUS Access Accept
- RADIUS Accounting Start
- RADIUS Accounting Interim
- RADIUS Accounting Stop

Depending on the customer needs, the session state repository can also be used to set session counters and limits. As such the session state repository can be required to keep a regional or global single view of all the actives sessions.

3. Solutions

Blue Print Solutions

Nokia AAA/AUS Can be deployed with a standard configuration in support of Blueprint Solutions that are maintained and updated by the core Noika AAA/AUS R&D team. The following section offers details of the current three standard Blueprint solutions.

3.1 AAA - LTE Blueprint

LTE (Long Term Evolution), marketed as 4G LTE, is a standard for wireless communication of high-speed data for mobile phones and data terminals. It is based on the GSM/EDGE and UMTS/HSPA network technologies, increasing the capacity and speed using new modulation techniques. Nokia AAA's LTE support offers wireless providers an economical CAPEX migration strategy to LTE that leverages existing network assets to enable seamless IP mobility between evolved 3G and LTE based on 3GPP R14 Standards. Nokia AAA supports LTE R16.x for Nokia AAA requirements

.

The 3GPP Reference Points currently supported by Nokia AAA are:

S6b

Diameter application for LTE

STa

Support of STa for Interworking with LTE networks

SWa

Support of SWa for Interworking with LTE networks

SWm

Support of SWm for Interworking with LTE networks

SWx

Support of SWx for Interworking with LTE networks

The TWAN TSCM use case is added to the standard LTE Policyflow in release 10.0

This feature allows for a rapid configuration of the Standards defined Trusted WLAN Access Network (TWAN) operating in Transparent Single Connection Mode (TSCM).

The authentication and authorization of users accessing trusted networks take place over STa, per 3GPP. This feature will add support to the STa interface for user access to a TWAN.

Voice over WiFi

Nokia AAA can also support untrusted access for the VoWiFi solution. Support for this solution includes:

- A SWm Diameter interface to ePDG to enable the ePDG to setup an IPsec tunnel to the UE
- A Diameter SWx interface to the HSS to retrieve subscriber credentials,
- A Diameter S6b interface to the Packet Gateway, and
- An optional Diameter SWa interface to the entitlement server. I
- PV4 and IPV6 support
- Emergency call Handling – 3GPP 14

WiFi and WiFi Offload

Nokia AAA supports end device access authentication for connections to a WiFi 802.1x network using the EAP authentication framework. In addition, a new WiFi Offload solution is available to allow for 3G offloading of end users toward WiFi hotspots. For release 8.1, support for HotSpot 2.0 Release 1 has been added to the product. This feature includes support for location information as per RFC 5580, enhancements to the existing EAP-TLS and EAP-TTLS plug-ins and test tools to support client Certificate Status Request Extension in TLS handshake (OCSP stapling) as described in IETF RFCs 5216 and 5281. In Release 9.0, Nokia AAA has implemented support for HotSpot 2.0, Release 2. In release 2, the following functionality was added to the product:

a) WFA Anonymous EAP-TLS
b) OCSP Stapling in TLS based EAP types
c) WFA HS2.0 Vendor Specific Attributes

- EAP-SIM/EAP-AKA protocols are supported for device authentication by
- Leverage existing authentication infrastructure
- Authentication prior to DHCP session
- Subscriber DHCP session created in WLAN Gateway

3.2 AAA - FEMTO Blueprint

A Femtocell or Femto network is a personal base station situated inside the building of the subscriber, within a small business premise, or a public place.

A Femtocell network typically provides network coverage to subscribers situated within a building, where large macro cells do not provide consistent coverage. Femtocells are also used in areas where there is not enough spectrum to meet the needs of subscribers. For example, a large number of subscribers share the total available data capacity in a macrocell base station. This reduces the data throughput available to an individual subscriber. This reduction in data throughput degrades the mobile broadband internet experience of an individual subscriber.

With Femtocell, service providers are able to reduce the amount and cost of the equipment needed for in-home wired and wireless access. Consumers gain low cost, flexible solutions which allow for improved mobile coverage, handset transparency, and the availability of high quality, enhanced services.

A Femtocell provides targeted coverage and can significantly increase the bandwidth available to a mobile within its field of operation. The Femtocell or Home Node B (HNB) supports the standard Universal Mobile Telecommunications System (UMTS) air interface. Femtocell provides cellular coverage in the home of a subscriber or a small business unit, and connects back to the core network of the service provider through a broadband IP network.

This section describes the major nodes and connections in a Femtocell network, and the role of these components in meeting the objectives of the mobile subscribers and operators. The Figure

The following is a workflow of the Femto network:

The Femto Base Station Router (BSR) includes the base station and the controller.

The Femto BSR connects back to the mobile operator core network for central authentication and management.

The SeGW is the security gateway. It connects to the AAA to authenticate the connecting Femtocell device.

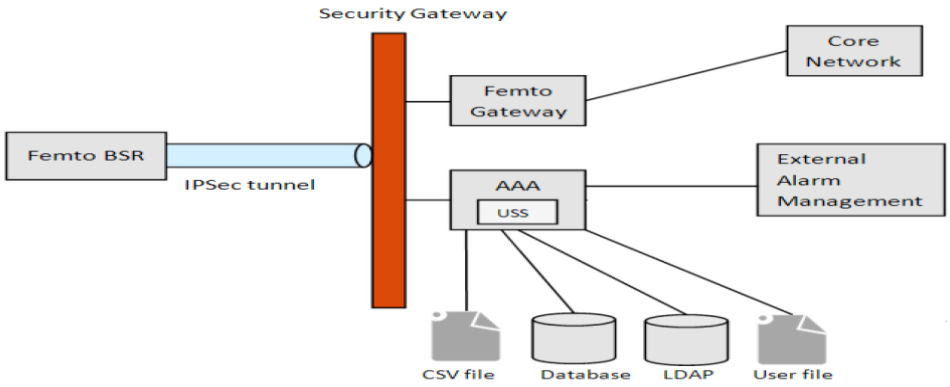

Figure 2

To authenticate users, AAA retrieves subscriber information from an internal or external

Data store which could include the following types of datastores: Lightweight Directory Access Protocol (LDAP), CSV delimited file, AAA user file.

In the Femtocell network, AAA performs the following tasks:

- Supports the proprietary EAP-DS2460, and Femto-Authorize-Only authentication methods to authenticate and authorize the Femto Access Point (FAP) against one of the specified Femtocell provisioning systems.
- Keeps track of the accounting data through Call Data Record (CDR) files.
- Interfaces with external databases, LDAP servers, and other servers to authenticate and
- Authorize Femto endpoint devices. These external servers store authentication details about users, authorization profiles, and blacklisted user data.

- If blacklist verification is enabled, then AAA also performs blacklist verification of the Femto AccessPoint.
- If configured, AAA performs whitelisting for Subject Key Id (SKI), Factory Serial Number (FSN), and National Location Lock (NLL).
- If configured, AAA supports sending the internal tunnel IP address as part of the authorization profile.
- If configured, AAA reports application alarms through Simple Network Management Protocol (SNMP) traps to the external alarm management system.

3.3 AUS - AUSF Blueprint

Nokia AUS provides the Authenticate service as defined in 3GPP TS 23.501 during the 5G access registration procedure. Upon request from the AMF, the AUSF executes authentication of the UE. Depending on the information provided by the AMF, the AUSF enters in one of the following procedures: 5G-AKA or EAP-based authentication'. The AUSF selects a UDM and gets the authentication data from UDM. Once the UE has been authenticated the AUSF provides relevant security related information to the AMF. In case the AMF provided a SUCI to AUSF, the AUSF shall return the SUPI to AMF only after the authentication is successful.

The AAA AUSF blue print solution supports N12 and N13. N13 to the UDM (Unified Data Management retrieves authentication vectors (SWx:MAR – like) and N12 interface to the AMF(Access and Mobility management Function). This is similar to LTE's STa/SWm/S6a all wrapped into one. The AUSF interfaces uses HTTPS2.0 instead of Diameter, AAA is equipped the ability to define HTTPS2.0 interfaces in Policyflow.

The AUSF Microservice will be supported with the following platform features:

- LCM of the Nokia AUS services via ZTS
- LOGs support on the Nokia AUS through ZTS
- CM of the Nokia AUS via ZTS
- ZTS integration for PM
- ZTS integration for FM
- Nokia AUS Backup / Restore by ZTS
- Support of secured gRPC interfaces
- AUSF integration with ZTS Secret Store service
- Nokia AUSF product development on ComPaaS lab (KPI-6.1)
- Functional testing of the Nokia AUS on ComPaaS (KPI-6.2)
- Demonstrate Cloud Native principles for the Nokia AUS (KPI-3)
- CSF KPI-2 - DevOps: CI build pipeline, SW stored in Artifactory, Automated tests
- 5G AUSF: Load Balancer on the N12 interface
- Nokia AUS-AUSF deployment on NCM + CLCM (Openstack)

The Nokia AUSF supports the following features in alignment with the 3GPP Service Based Architecture (SBA) support as defined in 23.501/23.502:

- Support of 5G AKA.
- Support of EAP-AKA': act as backend authentication server as per RFC 3748, RFC 5448 and Annex F of 33.501.

- Key derivation KSEAF from KAUSF.
- Synchronization failure recovery.
- Check SEAF authorization for the serving network name as received from the SEAF, respond with "serving network not authorized" in the Nausf_UEAuthentication_Authenticate response if there is no permission.
- Verification of the authentication response as received from SEAF, and error handling in case of no success. Support temporary storage of the RES* and expiry timer.
- For 5G AKA, the verification is optional (depending on VPLMN) via configuration.
- Support increased home control by providing the authentication result towards UDM via Nudm_UEAuthentication_ResultConfirmation Request to be used for further reaction (e.g. reject Registration of the UE).
- De-concealed SUPI as received from UDM/SIDF function is provided to SEAF after successful authentication only.

The following flow depicts the 5G AKA authentication to be supported by Nokia AUSF:

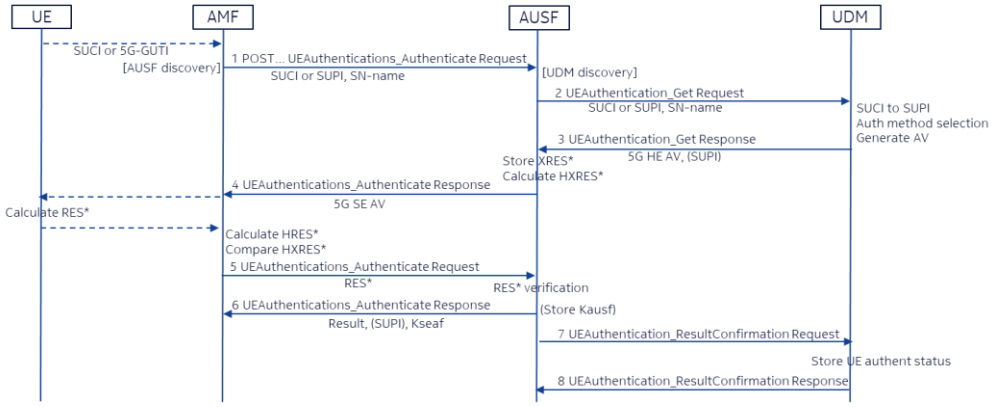

Figure 3

The Nokia AUSF will support the following features:

- New authentication algorithms can be added with a policy flow update.
- New authentication protocols/procedures can be added with a policy flow update.
- Overload control mechanisms.
- The Nokia AUSF UEAuth service is stateless, transaction-based, and can be N+k scaled independently of the other NF services.

4. References

5. Glossary

6. Appendix