RATS
Internet-Draft
Intended status: Informational
Expires: September 8, 2020

M. Chen
Li. Su
China Mobile

March 7, 2020

Use Cases for RATS
draft-chen-rats-usecase-00

Abstract

This document presents two demand scenarios from the Internet Service Providers' perspective as an supplement use case of the RATS work group. And make some discussions from the two dimensions of access authentication and application authentication.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 8, 2020.

Table of Contents

1. Introduction

At present, it is necessary to complete the authentication before accessing the operator's network to obtain the service. RATS aimed at the solutions to provide interoperable way for domain-specific attestation mechanisms, within RATS relying party may not to maintain the authentication background, as an ISP what may be involved at the level of access authentication is preshared secret keys based authentication, the authentication based on PSK(Preshared secret keys) is different from identity-based authentication, such as IBC(Identity-Based Cryptograph).

After access to the network, operators can also provide application layer authentication services for a variety of applications. At present, there are many application layer authentication methods, it can be divided into certificate-based and non-certificate-based certification systems, so there are the following situations. One application authenticated by certificate-based PKI system may request resource access to a server or service, but the server or service's authentication function is based on identity which is belong to non-certificate-based certification systems. These are all possible future demand scenarios, also in the context of the RATS. Due to limitation of resource, many companies are unable to operate their own certification and willing to rely on the result from operator to reduce their cost, and operator can provide authentication services. Multiple certification centers would be made due to different kinds of request from service and perspective of deployment, before obtaining a certification center's service, certification center need proof for identification, including software and hardware health information. These certification centers are based on regions then there have manage barriers, how can clients from a certification center asstest themselves' identities to another certification center. Especially now there are more virtual resources, cloud resources, one need to prove whether it has access to the resources and can protect the data. From an internal business perspective, how

to integrate resources, achieve cross-domain trust and break down management barriers in order to streamline and improve flexibility will also be something rats[I-D.ietf-rats-architecture] can do.

2. Terminology

The readers should be familiar with the terms defined in.

In addition, this document makes use of the following terms:

PSK: Preshared secret keys means keys are shared in advance between the authentication parties.

IBC: Identity-Based Cryptograph, it is an asymmetric public key cryptosystem.

PKI: Public Key Infrastructure, an infrastructure built with a public-key mechanism.

3. Use Cases

This section describes use cases which happens inside an ISP.

3.1. Access authentication based on different method

This section considers the level of access authentication. For operators, the access of users is usually based on preshared secret keys, preset with symmetric secret keys before the release. The first access only needs to be activated, and subsequent authentication uses PSK to complete data protection which is based on Symmetric secret key system. In addition, there are other identity-based authentication methods, the access authentication based on identity is asymmetric and the identity is the public key, this approach makes it easier for the peer to obtain the public key of the other peer.

In short, these are two different authentication methods. When a psk-based authentication device needs to request an identity-based service, it needs to prove its' trustworthiness to the other party and the whole process need to ensure the confidentiality of evidences and attestation results.

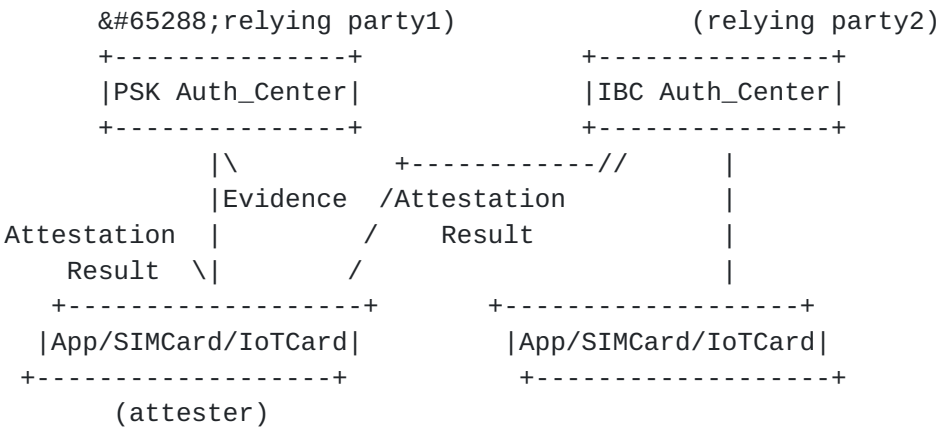

Figure 1: different access authentication methods within RATS

The format and content of the evidence: TBD

The format of the Attestation Result: TBD

The transmission protocol for evidence or attestation result: TBD

3.2. Application authentication based on different system

At the application level, due to limitation of resource, many applications need operators to provide business authentication services. At present, there are two business authentication methods: one is certification-based PKI system authentication, because the management of certificates is always a very big problem, so the other is non-certificated, such as identity-based authentication whose identity is readable.

When cross-business authentication is required, how to prove one's identity to the other will be a common problem.

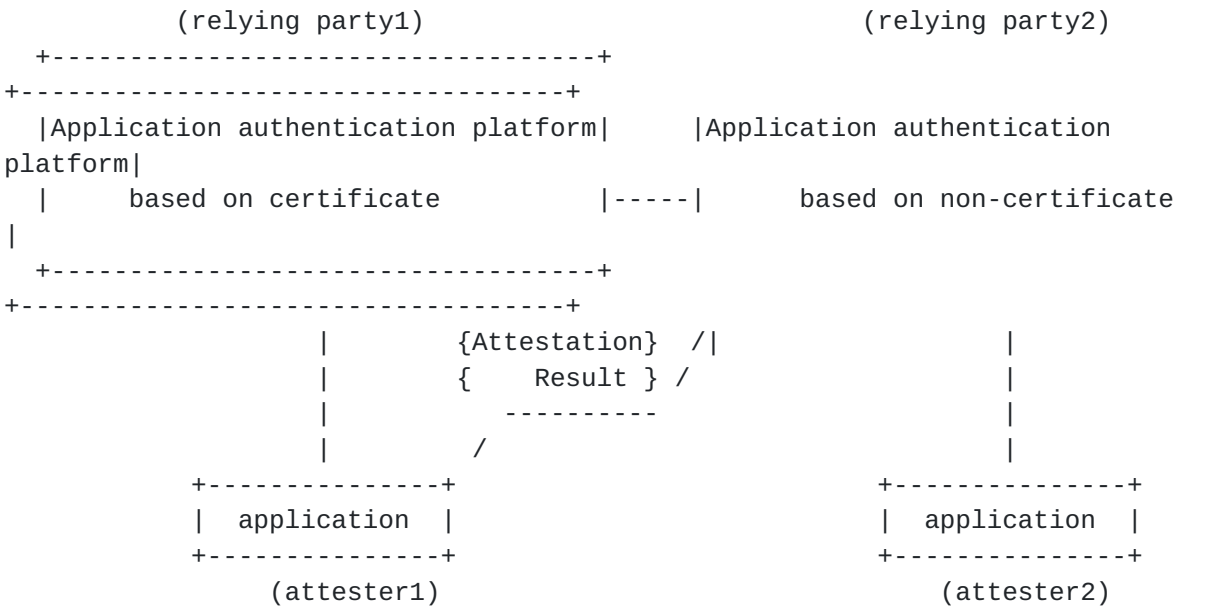

Figure 2: different application authentication methods in RATS architecture

The format and content of the evidence: TBD

The format of the Attestation Result: TBD

The transmission protocol for evidence or attestation result: TBD

Certification-based authentication process: TBD

Identity-based authentication process: TBD

4. Security Considerations

TBD

5. IANA Considerations

This document does not require any action from IANA.

6. Acknowledgement

TBD

7. Informative References

[I-D.ietf-rats-architecture]
Birkholz, H., Thaler, D., Richardson, M., Smith, N., and W. Pan, "Remote Attestation Procedures Architecture", draft-ietf-rats-architecture-02 (work in progress), March 2020.

Authors' Addresses

Meiling Chen
China Mobile
32, Xuanwumen West
BeiJing, BeiJing 100053
China

Email:
chenmeiling@chinamobile.com

Li Su
China Mobile

32, Xuanwumen West

BeiJing

100053

China

Email:
suli@chinamobile.com