Workgroup: RATS Working Group
Internet-Draft: draft-ietf-rats-daa-02
Published: 7 September 2022
Intended Status: Informational
Expires: 11 March 2023
Authors: H. Birkholz   C. Newton
Fraunhofer SIT   University of Surrey
L. Chen   D. Thaler
University of Surrey   Microsoft

Direct Anonymous Attestation for the Remote Attestation Procedures Architecture

Abstract

This document maps the concept of Direct Anonymous Attestation (DAA) to the Remote Attestation Procedures (RATS) Architecture. The role DAA Issuer is introduced and its interactions with existing RATS roles is specified.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-rats-daa/.

Discussion of this document takes place on the Remote ATtestation ProcedureS (rats) Working Group mailing list (mailto:rats@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/rats/.

Source for this draft and an issue tracker can be found at https://github.com/ietf-rats-wg/draft-ietf-rats-daa.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Remote ATtestation procedureS (RATS, [I-D.ietf-rats-architecture]) describe interactions between well-defined architectural constituents in support of Relying Parties that require an understanding about the trustworthiness of a remote peer. The identity of an Attester and its corresponding Attesting Environments play a vital role in RATS. A common way to refer to such an identity is the Authentication Secret ID as defined in the Reference Interaction Models for RATS [I-D.ietf-rats-reference-interaction-models]. The fact that every Attesting Environment can be uniquely identified in the context of the RATS architecture is not suitable for every application of remote attestation. Additional issues may arise when Personally identifiable information (PII) -- whether obfuscated or in clear text -- are included in attestation Evidence or even corresponding Attestation Results. This document illustrates how Direct Anonymous Attestation (DAA) can mitigate the issue of uniquely (re-)identifiable Attesting Environments. To accomplish that goal, a new RATS role -- the DAA Issuer -- is introduced and its duties as well as its interactions with other RATS roles are specified.

2. Terminology

This document uses the following set of terms, roles, and concepts as defined in [I-D.ietf-rats-architecture]: Attester, Verifier, Relying Party, Conceptual Message, Evidence, Attestation Result, Attesting Environment. The role of Endorser, also defined in [I-D.ietf-rats-architecture], needs to be adapted and details are given below.

Additionally, this document uses and adapts, as necessary, the following concepts and information elements as defined in [I-D.ietf-rats-reference-interaction-models]: Attester Identity, Authentication Secret, Authentication Secret ID

A PKIX Certificate is an X.509v3 format certificate as specified by [RFC5280].

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**NOT RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Direct Anonymous Attestation

Figure 1 shows the data flows between the different RATS roles involved in DAA.

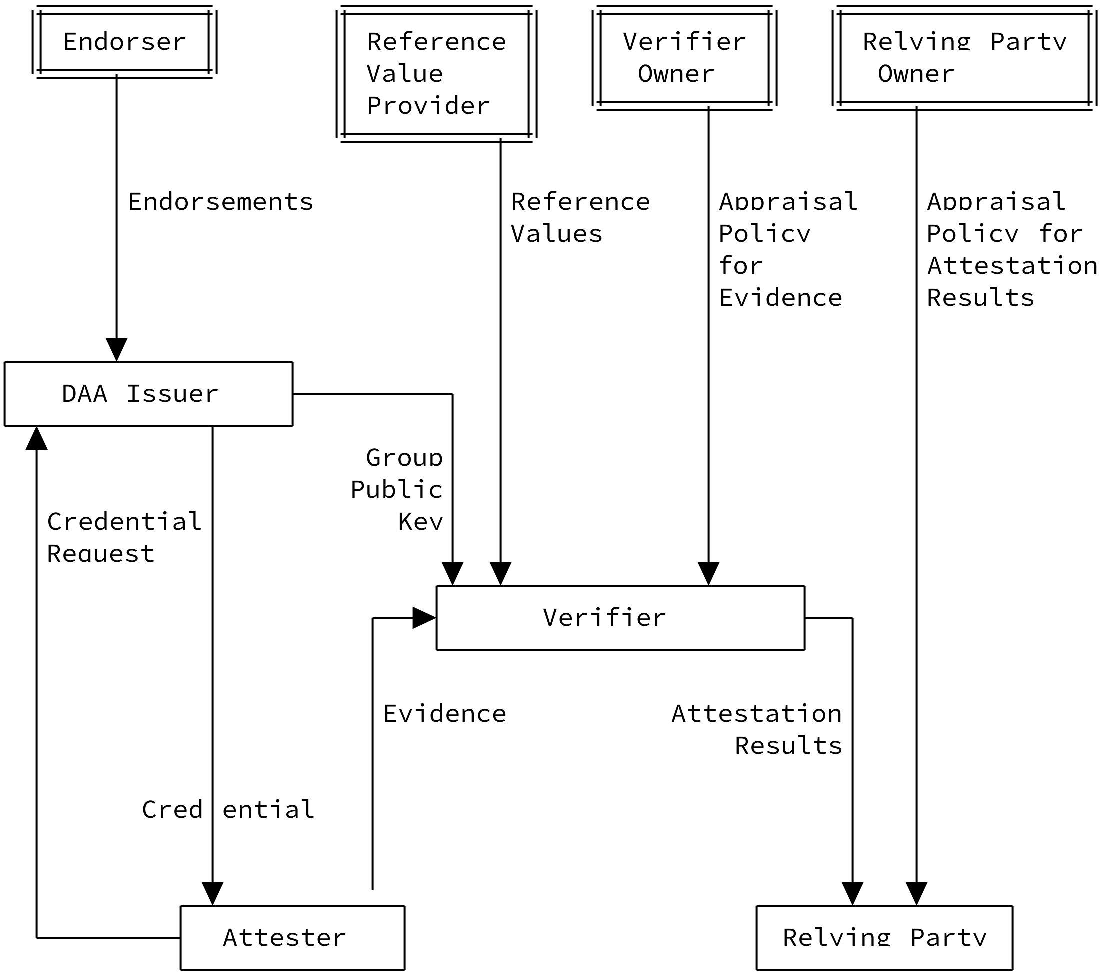

Figure 1: DAA data flows

DAA [DAA] is a signature scheme that allows the privacy of users that are associated with an Attester (e.g. its owner) to be maintained. Essentially, DAA can be seen as a group signature scheme with the feature that given a DAA signature no-one can find out who the signer is, i.e., the anonymity is not revocable. To be able to sign anonymously, an Attester has to obtain a credential from a DAA Issuer. The DAA Issuer uses a private/public key pair to generate credentials for a group of Attesters and makes the public key (in the form of a public key certificate) available to the verifier in order to enable them to validate the Evidence received.

In order to support these DAA signatures, the DAA Issuer **MUST** associate a single key pair with a group of Attesters and use the same key pair when creating the credentials for all of the Attesters in this group. The DAA Issuer's group public key certificate replaces the individual Attester Identity documents during authenticity validation as a part of the appraisal of Evidence conducted by a verifier. This is in contrast to intuition that there has to be a unique Attester Identity per device.

For DAA, the role of the Endorser is essentially the same, but they now provide Attester endorsement documents to the DAA Issuer rather than directly to the verifier. These Attester endorsement documents enable the Attester to obtain a credential from the DAA Issuer.

4. DAA changes to the RATS Architecture

In order to enable the use of DAA, a new conceptual message, the Credential Request, is defined and a new role, the DAA Issuer role, is added to the roles defined in the RATS Architecture.

Credential Request: An Attester sends a Credential Request to the DAA Issuer to obtain a credential. This request contains information about the DAA key that the Attester will use to create evidence and, together with Attester endorsement information that is provided by the Endorser, to confirm that the request came from a valid Attester.

DAA Issuer: A RATS role that offers zero-knowledge proofs based on public-key certificates used for a group of Attesters (Group Public Keys) [DAA]. How this group of Attesters is defined is not specified here, but the group must be large enough for the necessary anonymity to be assured.

Effectively, these certificates share the semantics of Endorsements, with the following exceptions:

- Upon receiving a Credential Request from an Attester, the associated group private key is used by the DAA Issuer to provide the Attester with a credential that it can use to convince the Verifier that its Evidence is valid. To keep their anonymity, the Attester randomises this credential each time that it is used. Although the DAA Issuer knows the Attester Identity and can associate this with the credential issued, randomisation ensures that the Attester's identity cannot be revealed to anyone, including the DAA Issuer.

- The Verifier can use the DAA Issuer's group public key certificate, together with the randomised credential from the Attester, to confirm that the Evidence comes from a valid Attester without revealing the Attester's identity.

- A credential is conveyed from a DAA Issuer to an Attester in combination with the conveyance of the group public key certificate from DAA Issuer to Verifier.

5. Additions to Remote Attestation principles

In order to ensure an appropriate conveyance of Evidence via interaction models in general, the following prerequisite considering Attester Identity **MUST** be in place to support the implementation of interaction models.

Attestation Evidence Authenticity: Attestation Evidence **MUST** be correct and authentic.

In order to provide proofs of authenticity, Attestation Evidence **SHOULD** be cryptographically associated with an identity document that is a randomised DAA credential.

The following information elements define extensions for corresponding information elements defined in [I-D.ietf-rats-reference-interaction-models], which are vital to all types of reference interaction models. Varying from solution to solution, generic information elements can be either included in the scope of protocol messages (instantiating Conceptual Messages defined by the RATS architecture) or can be included in additional protocol parameters of protocols that facilitate the conveyance of RATS Conceptual Messages. Ultimately, the following information elements are required by any kind of scalable remote attestation procedure using DAA with one of RATS's reference interaction models.

Attester Identity ('attesterIdentity'): *mandatory*

In DAA, the Attester's identity is not revealed to the verifier. The Attester is issued with a credential by the DAA Issuer that is randomised and then used to anonymously confirm the validity of their evidence. The evidence is verified using the DAA Issuer's group public key.

Authentication Secret IDs ('authSecID'): *mandatory*

In DAA, Authentication Secret IDs are represented by the DAA Issuer's group public key that **MUST** be used to create DAA credentials for the corresponding Authentication Secrets used to protect Evidence.

In DAA, an Authentication Secret ID does not identify a unique Attesting Environment but is associated with a group of Attesting Environments. This is because an Attesting Environment should not be distinguishable and the DAA credential which represents the Attesting Environment is randomised each time it used.

6. Privacy Considerations

As outlined above, for DAA to provide privacy for the Attester, the DAA group must be large enough to stop the Verifier identifying the Attester.

Randomisation of the DAA credential by the Attester means that collusion between the DAA Issuer and Verifier, will not give them any advantage when trying to identify the Attester.

For DAA, the Attestation Evidence conveyed to the Verifier **MUST** not uniquely identify the Attester. If the Attestation Evidence is unique to an Attester other cryptographic techniques can be used, for example, property based attestation [PBA].

7. Security Considerations

The anonymity property of DAA makes revocation difficult. Well known solutions include:

1. Rogue Attester revocation -- if an Attester's private key is compromised and known by the Verifier then any DAA signature from that Attester can be revoked.

2. EPID - Intel's Enhanced Privacy ID -- this requires the Attester to prove (as part of their Attestation) that their credential was not used to generate any signature in a signature revocation list.

There are no other special security considerations for DAA over and above those specified in the RATS architecture document [I-D.ietf-rats-architecture].

8. Implementation Considerations

The new DAA Issuer role can be implemented in a number of ways, for example:

1. As a stand-alone service like a Certificate Authority, a Privacy CA.

2. As a part of the Attester's manufacture. The Endorser and the DAA Issuer could be the same entity and the manufacturer would then provide a certificate for the group public key to the Verifier.

9. IANA Considerations

We don't yet.

10. References

10.1. Normative References

[DAA] Brickell, E., Camenisch, J., and L. Chen, "Direct anonymous attestation", DOI 10.1145/1030083.1030103, Proceedings of the 11th ACM conference on Computer and communications security - CCS '04, 2004, <https://doi.org/10.1145/1030083.1030103>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

10.2. Informative References

[I-D.ietf-rats-architecture] Birkholz, H., Thaler, D., Richardson, M., Smith, N., and W. Pan, "Remote Attestation Procedures Architecture", Work in Progress, Internet-Draft, draft-ietf-rats-architecture-21, 16 August 2022, <https://www.ietf.org/archive/id/draft-ietf-rats-architecture-21.txt>.

[I-D.ietf-rats-reference-interaction-models] Birkholz, H., Eckel, M., Pan, W., and E. Voit, "Reference Interaction Models for Remote Attestation Procedures", Work in Progress, Internet-Draft, draft-ietf-rats-reference-interaction-models-05, 26 January 2022, <https://www.ietf.org/archive/id/draft-ietf-rats-reference-interaction-models-05.txt>.

[PBA] Chen, L., Löhr, H., Manulis, M., and A. Sadeghi, "Property-Based Attestation without a Trusted Third Party", DOI 10.1007/978-3-540-85886-7_3, Lecture Notes in Computer Science pp. 31-46, September 2008, <https://doi.org/10.1007/978-3-540-85886-7_3>.

Authors' Addresses

Henk Birkholz
Fraunhofer SIT
Rheinstrasse 75
64295 Darmstadt
Germany

Email: henk.birkholz@sit.fraunhofer.de

Christopher Newton
University of Surrey

Email: cn0016@surrey.ac.uk

Liqun Chen
University of Surrey

Email: liqun.chen@surrey.ac.uk

Dave Thaler
Microsoft
United States of America

Email: dthaler@microsoft.com